CYBERSECURITY PEDAGOGY & PRACTICE JOURNAL

Volume 1, No. 1
July 2022
ISSN: 2832-1006

In this issue:

iscap
Information Systems & Computing Academic Professionals

The **Cybersecurity Pedagogy and Practice Journal** (**CPPJ**) is a double-blind peer-reviewed academic journal published by **ISCAP** (Information Systems and Computing Academic Professionals). Publishing frequency is two times per year. The first year of publication was 2022.

CPPJ is published online (https://cppj.info). Our sister publication, the proceedings of the ISCAP Conference (https://proc.iscap.info) features all papers, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the ISCAP conference. At that point papers are divided into award papers (top 15%), and other accepted proceedings papers. The other accepted proceedings papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the CPPJ journal. Currently the target acceptance rate for the journal is under 35%.

Questions should be addressed to the editor at editorcppj@iscap.us or the publisher at publisher@iscap.us. Special thanks to members of ISCAP who perform the editorial and review processes for CPPJ.

2022 ISCAP Board of Directors

CYBERSECURITY PEDAGOGY AND PRACTICE JOURNAL

Editors

Teaching Case

Rubber Duckies in the Wild: Proof of Concept Lab for USB Pen Testing Tool

Anthony Serapiglia
Saint Vincent College, Latrobe, PA, 15650
Anthony.Serapiglia@stvincent.edu

Abstract

Ethical Hacking has matured into a widely accepted and necessary part of the cybersecurity world. Actively probing and testing the defenses of a network or business system is essential to maintaining CIA benchmarks of Confidentiality, Integrity, and Availability. Penetration testing has evolved into a special subset of the industry. Companies and organizations of all sizes and across a range of industries rely on pen testers to proactively identify weakness in cyber-defenses before a real attack effects real damage. One of the primary objectives of penetration testers is the creation of a remote access shell into a system. A common method of achieving this is through the use of "rubber ducky" USB devices that, when inserted into a computing device, initiates an active session from inside a network to allow remote access to the pen tester. This teaching case provides background and instructions on incorporating a proof-of-concept rubber ducky build into an undergraduate cybersecurity course.

Keywords: Penetration Testing, Ethical Hacking, Cybersecurity, Rubber Ducky, White Hat Hacking

1. INTRODUCTION

NIST Special Publication 800-115 begins to define penetration testing (pen test) as "…security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network" (NIST, 2008).

Pen tests differ from standard vulnerability scanning. The end goal of the scanning is simply the identification of weak spots such as missing patches or outdated software versions. The final product is a report that may or may not be actionable. Pen testing goes further. As part of a thorough pen test, an attempt is made to exploit the vulnerabilities identified in scanning. This extra step is crucial to identifying the difference between theoretical vulnerabilities and ones that can be actively exploited. This allows a more precise classification of priorities in remediation. It also helps to get the attention of "C-Suite" or managerial decision makers who may not understand the urgency of the situation.

A good pen test should be performed by actors outside of the organization being tested. Thus, the testers do not subconsciously bring inside information to the table when executing their attacks. Very few people in an organization should know that a pen test is being performed. This helps to ensure that tests are performed under normal working conditions and that defenses have not been artificially raised for the occasion only to be dropped later.

Full pen tests encompass entire systems. This includes systems that are both inside an organization and possibly hosted elsewhere. Many times, a pen test will also include a test of physical security and surrounding systems, policies, and procedures. It has been a common theme of many organizations that much effort is placed on technical perimeter defenses for internet connected systems, but internal controls allowing for physical access to devices and networks remain a soft underbelly ripe for attack.

Critical to any pen test operation is that a set of ground rules be agreed upon by both parties prior to the test. Boundaries and scope of work must be declared. An emergency contact(s) must be in place in case anything would stray from the accepted field of play or if, as part of the response to a potential 'breach of security' event, personnel of the target company engage law enforcement. Someone must be available to notify those involved to stand down and that the test is an authorized exercise.

A case in Dallas County, Iowa in September of 2019 resulted in two employees of cybersecurity firm Coalfire Labs being arrested. While testing security at the county courthouse, the two performed a physical pen test, attempting to gain physical access to the courthouse. They had been engaged by Iowa's State Court Administration and had a written statement, or "get out of jail free card" with them, but the local sheriff proceeded to arrest both for felony third-degree burglary charges. They were released after a night in jail and posting $100,000 in bond. Charges were later reduced to misdemeanor trespassing. It was nearly a year until the charges were dropped after an education campaign and widespread publicity generated by the larger ethical hacking and cybersecurity community (Krebs, 2020; Osborne, 2020). Of the contributing factors in the misunderstanding, two stand out. First, the terms of the pen test agreement clearly stated that no doors should be forced open. The pen testers stated that they had entered through an unlocked front door. The Sheriff disagreed. Second, the contacts on the "get out of jail free" card were not able to be reached for verification at 12:30 in the morning to verify that the two were in fact cybersecurity contractors (Goodin, 2019).

2. RUBBER DUCKY

One of the many characteristics of an ethical hacker/pen tester is the ability to be creative and to become a "maker". After all, the evolution of the term hacker in the modern sense begins with a model train club at MIT (Levy, 1984) and grew through communities, "…who enjoy exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary (Yagoda, 2014).

An essential step in the maturation of a hacker is the ability to create their own tools. A hacker who is able to create and craft their own tools is one who recognizes the situation at hand, the environment and variables, and applies problem solving techniques to develop a solution that can cross from a virtual world of the theoretical and into the physical world of action. This is an area where practice can move from rote recipe to an evolving art. Not every attempt is guaranteed success. There may be some false starts. There will be troubleshooting and debugging. There may be frustration. There is value in frustration. Once a solution is achieved and a task accomplished, the greater the frustration the greater the reward.

A primary objective of penetration testers is the creation of a remote access shell from within the system. A common method of achieving this is through the use of "rubber ducky" USB devices that when inserted into computing services activate an active session from inside a network to allow remote access to the pen tester.

A USB rubber ducky is most commonly a keystroke injection tool disguised as a generic flash drive. Computers recognize it as a regular keyboard and automatically accept its pre-programmed keystroke payloads at over 1000 words per minute (Hak5, 2021).

The first rubber ducky hacking devices were drop keys, USB sticks that had been preprogrammed to deliver a payload when inserted into a computer. These devices were left in open spaces to be picked up by unsuspecting people, many of whom would plug them into a computer either to attempt to find the owner or for personal use. Many users still commonly log in and perform their daily functions on their computers utilizing an account with administrative privileges (Krebs, 2006; Burnette, 2020). This often allows executables to run without any further prompting or warning messages to the user. Rubber ducky drop keys essentially functioned as a message in a bottle floating randomly on the sea, with the difference being that the researcher did not have to rely on the finder to actively send a message back. Executing a program to phone home happened automatically.

As a pen tester, a more precise and direct targeting is both possible and expected. Gaining physical entry into a building, organization, or just an individual in a public space such as a coffee shop can allow a pen tester sufficient access to discretely insert a USB device and gain access to a computer. Heightened awareness and popularity of the directed use of a rubber ducky for hacking purposes was reached after being featured in the television series Mr. Robot in 2016. Commercial pre-programed rubber ducky devices are readily available and retail for price of $50. The material cost of the hardware to develop a rubber ducky can come in below $3 per unit. In many of the use cases, these devices become expendable and are not recaptured, making a compelling case for the DIY route.

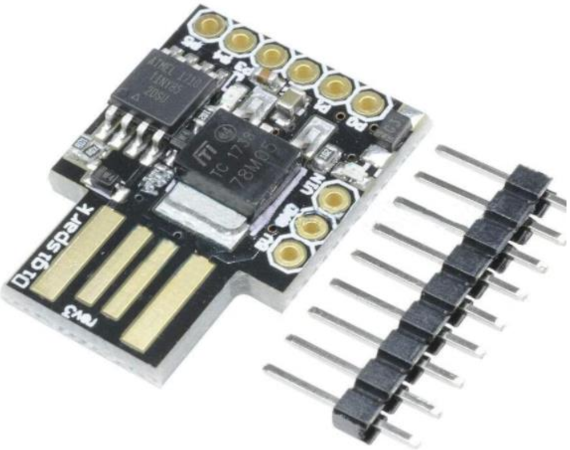


Figure 1: ATTINY85 controller

At the core of a rubber ducky is a programmable controller chip with a USB connector. This assignment will assume a common Digispark ATTINY85 for Arduino General Micro USB Development Board. In July of 2021, 5-piece packs of ATTINY85 controllers could be purchased for $13.99 (https://www.amazon.com/AITRIP-Digispark-Kickstarter-ATTINY85-Development/dp/B08HYHPTX2/).

3. ASSIGNMENT

Task

Create a droppable USB Rubber Ducky that when inserted into a Windows computer will create a text file on the user's desktop named "pwned.txt" and containing the text "Hello World – You have been pwned."

Ingredients

- Arduino IDE found at: (https://www.arduino.cc/en/software)
  The Arduino development environment is free, opensource, and available on Linux, Mac, and windows platforms.

- ATTiny85 (Digispark) USB Controller Board (generally available for purchase for approximately $3 or less per unit)

- Digispark driver (if necessary) can be found at: https://github.com/digistump/DigistumpArduino/releases

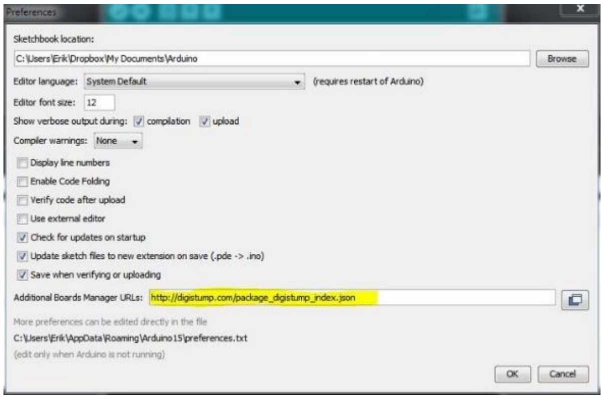
Getting Started

This exercise proceeds in the following order: setup of the development environment, programming of the device, testing the device, and deployment of the device.

Environment Setup

Follow instructions for Arduino IDE installation based on your operating system.

Post-installation, the IDE will need to be updated with a specific board manager for the ATTINY85. go to File -> Preferences. Next to "Additional Board Manager URLs:" enter: http://digistump.com/package_digistump_index.json



Preferences

Sketchbook location: C:\Users\Erik\Dropbox\My Documents\Arduino [Browse]

Editor language: System Default (requires restart of Arduino)

Editor font size: 12

Show verbose output during: ☑ compilation ☑ upload

Compiler warnings: None

☐ Display line numbers
☐ Enable Code Folding
☐ Verify code after upload
☐ Use external editor
☑ Check for updates on startup
☑ Update sketch files to new extension on save (.pde -> .ino)
☑ Save when verifying or uploading

Additional Boards Manager URLs: http://digistump.com/package_digistump_index.json

More preferences can be edited directly in the file
C:\Users\Erik\AppData\Roaming\Arduino15\preferences.txt
(edit only when Arduino is not running)

[OK] [Cancel]

Figure 2: Preference setting to add board manager in Arduino IDE

Once the URL is added, go to Tools > Board "Arduino Uno" > Boards Manager. In the textbox at the top, type Digispark and install the Digistump AVR Boards board manager.
If necessary, install Digispark device drivers.

Programming

A basic build of a beginner rubber ducky will program the ATTINY chip to be recognized as an HID (Human Interface device) when inserted, acting as a keyboard delivering keystroke input at up to 1000 words per minute.

Given the nature of the device, many possibilities exist for payload options. The ATTiny85 chip supports C, but is Arduino-compatible. Utilizing the Digispark board manager in the Arduino IDE opens a full range of natural language commands. DuckyScript was developed by Hak5 as a scripting language for their proprietary products. A community of developers have contributed many preconfigured scripts available through quick search efforts. Free online services such as the digiQuack DuckyScript convertor are also available to make these scripts usable in the Arduino environment (https://cedarctic.github.io/digiQuack/).

A basic script to complete the task of message creation for this assignment can be completed in less than 20 lines of code. Be creative. Experiment. Test and debug.

Testing and Deployment

As with any project related to penetration testing and ethical hacking, testing should be performed in a restricted and secured lab environment. Deployment of this device should only be done under instructor guidance, or under contract with explicit boundaries stated.

4. CONCLUSION

Becoming a pen tester requires a full spectrum of knowledge and skills inside and outside of technology. The after-action reports of pen testers can read like movie scripts. It is an exciting and thrilling area of cybersecurity that is unlike any other. One of the features that sets pen testing apart from other areas of cybersecurity is the crossover into the real world. Full pen testing often encompasses in-person physical exploitation of work environments. Field work is unpredictable, and success depends on flexibility, adaptability, and a full set of tools.

The USB Rubber Ducky has taken many forms recently; from experiments on seeding an environment with innocuous flash drives to see if one is randomly picked up to phone home, to Swiss Army knives full of exploitable packages deployed with precision by a pen tester in person. Most use cases for a ducky involve leaving it behind, with a low percentage chance of recovery.

It has been a legacy of many professions that one of the signs of an apprentice maturing into a master is the ability to create their own tools. This step forward shows that the neophyte understands the greater depth of their environment, the specific task or problem to be solved as well as the exact tool necessary to solve it. It also shows the command of the resources available to them in the creation of a suitable tool for the task.

Including labs that require beginning cybersecurity students to create their own tools helps to foster this progress in them. It synthesizes the various and multiple technologies together. It provides a springboard to further creative projects that bring the individual building blocks together after experiencing the initial success in building a foundational platform for direct use in real world exploitation.

5. REFERENCES

Burnette, M. (2020, January 23). Why You Should Not Use an Admin Account. Retrieved May 21, 2021, from https://www.lbmc.com/blog/why-you-should-not-use-an-admin-account/

Goodin, D. (2019, November 13). How a turf war and a botched contract landed 2 pentesters in Iowa jail. Retrieved February 9, 2021, from https://arstechnica.com/information-technology/2019/11/how-a-turf-war-and-a-botched-contract-landed-2-pentesters-in-iowa-jail/

Hak5, LLC. (n.d.). USB RUBBER DUCKY. Retrieved April 21, 2021, from https://docs.hak5.org/hc/en-us/categories/360000982554-USB-Rubber-Ducky

Krebs, B. (2006, April 18). Windows Users: Drop Your Rights. Retrieved July 11, 2021, from http://voices.washingtonpost.com/securityfix/2006/04/windows_users_drop_your_rights.html

Krebs, B. (2020, January 31). Iowa Prosecutors Drop Charges Against Men Hired to Test Their Security. Retrieved June 12, 2021, from https://krebsonsecurity.com/2020/01/iowa-prosecutors-drop-charges-against-men-hired-to-test-their-security/

Levy, S. (2014, November 21). The Tech Model Railroad Club. Retrieved March 3, 2021, from https://www.wired.com/2014/11/the-tech-model-railroad-club/

Osborne, C. (2020, February 03). Charges dropped against Coalfire security team who broke into courthouse during pen test. Retrieved June 12, 2021, from https://www.zdnet.com/article/charges-dropped-against-penetration-testers-who-broke-into-courthouse/

Scarfone, K., Souppaya, M., Cody, A., Orebaugh, A. (September, 2008). Technical Guide to Information Security Testing and Assessment, NIST Computer Security Resource Center Special Publications 800-115. Retrieved February 16, 2021, from Technical guide to information security testing and assessment (nist.gov)

Yagoda, B. (2014, March 06). A Short History of "Hack". Retrieved March 3, 2021, from https://www.newyorker.com/tech/annals-of-technology/a-short-history-of-hack.