.... The Digispark Attiny85 Rubber Ducky ....

A

Project Synopsis

Submitted

In partial fulfilment

For the award of the Degree of

Bachelor of Technology

In Department of Computer Science Engineering

Submitted To

Mr Govind Singh

H.O.D. (EE)

Submitted By

Name of Candidate:
Awanish,Vinay, Niraj
Enrolment No

Department of Computer Science Engineering

CHARTERED INSTITUTE OF TECHNOLOGY, ABUROAD

Bikaner Technical University, Bikaner

April 2023

ABSTRACT

The Digispark Attiny85 Rubber Ducky Attack is a technique used to exploit computer systems by emulating a USB keyboard. It involves using a small device to simulate keyboard input and execute pre-programmed scripts to automate actions on the target system. The technique can be used for malicious purposes, such as gaining remote access or stealing sensitive data, or for ethical purposes, such as testing security systems.

The Digispark Attiny85 Rubber Ducky Attack is easy to carry out and requires minimal technical knowledge or experience. Organizations can protect against this technique by implementing USB device controls, disabling USB ports, and regularly updating system software.

Project Description:-

INTRODUCTION

The Digispark Attiny85 Rubber Ducky Attack is a powerful and popular technique used to exploit computer systems by emulating a USB keyboard. The technique involves using a small device, such as the Digispark Attiny85, to simulate keyboard input and execute pre-programmed scripts that can automate a range of actions on the target system. This technique can be used for a variety of purposes, such as gaining remote access, stealing sensitive data, or compromising security systems. With the Digispark Attiny85 Rubber Ducky Attack, even a novice attacker can quickly and easily carry out sophisticated attacks without any technical knowledge or experience. However, it is important to note that this technique can also be used for ethical purposes, such as testing the security of computer systems or demonstrating potential vulnerabilities to organizations.

OBJECTIVES

The Digispark Attiny85 Rubber Ducky Attack refers to a security vulnerability in which an attacker can use a Digispark Attiny85 microcontroller to emulate a USB keyboard and execute arbitrary commands on a target computer.

The vulnerability arises due to the Digispark's ability to reprogram itself to act as a USB human interface device (HID), which is the same interface used by keyboards and mice to communicate with computers. By default, the Digispark is programmed to act as a USB device, but an attacker can reprogram it to act as a keyboard and execute any pre-determined set of commands on the target computer, without the user's knowledge.

This vulnerability can be exploited in a variety of ways, such as to steal sensitive information, install malware or backdoors, or to escalate privileges on the target system. As a result, the Digispark Attiny85 Rubber Ducky Attack poses a significant risk to the security of computers and information systems.

METHODOLOGY

A Digispark Arduino Rubber Ducky can be a useful tool for pentesters, as it can be used to automate certain tasks and launch various types of attacks on a target system. Here are a few examples of problems that a Digispark Arduino Rubber Ducky can help solve for pentesters:

- Automating tasks
- Social engineering attacks
- Physical access attacks
- Bypassing security controls
- Exploiting vulnerabilities

INNOVATION AND CONTRIBUTION TO THE FIELD

The Digispark Attiny85 Rubber Ducky Attack project has the potential to make significant contributions to the field of cybersecurity by identifying a previously unknown vulnerability and developing mitigation strategies to protect against it. The project's innovation lies in its identification of the Digispark microcontroller as a potential vector for keyboard emulation attacks, and its development of a proof-of-concept attack to demonstrate the vulnerability.

Team members:- Awanish Chaurasiya, Vinay Gurjar, Niraj Charan

Time Duration:- The Total Duration of this project is expected to be 1 month , starting fromthe date of approval. The project timeline is broken down into the following steps:-

- **Week 1: Research and planning**
  ->Conduct research on rubber ducky tools and how they work.
  ->Gather information on Scripts and how they function.
  ->Plan the design and implementation of the project.
  ->Create a list of necessary components and tools.
  ->Order or purchase any required components.

- **Week** 2: Setup andtesting
  ->Set up the development environment and install required software.
  ->Test the Digispark board and ensure that it is functioning correctly.
  ->Develop and test the scripts/Sketches.
  ->Test the script on a test machine to ensure that it is working properly.

- **Week 3:** Finalize Script and Hardware Integration
  ->Make any necessary changes to the script based on testing.
  ->Integrate the script with the Digispark board.
  ->Test the integration and troubleshoot any issues that arise.
  ->Finalize the design of the rubber ducky tool.

- **Week** 4: Documentation and Presentation Preparation
  ->Write the documentation for the project, including a detailed explanation of the project, its purpose, and its functionality.
  ->Create a presentation to showcase the project.
  ->Test the final version of the project to ensure that everything is working properly.
  ->Prepare for the presentation and practice delivering it.

Problem Statement:

Develop an ethical hacking tool to test the security measures of computer systems by attempting to bypass existing defenses.

Future Scope:

1. Expand the tool's capabilities to include testing for specific types of vulnerabilities, such as network vulnerabilities or software vulnerabilities.

2. Develop a reporting module within the tool to generate detailed reports of vulnerabilities identified during the testing process. The reports can help organizations identify potential areas of improvement and prioritize remediation efforts.

3. Integrate the tool with existing security information and event management (SIEM) solutions to provide real-time alerts and notifications when potential security breaches occur.

4. Integrate the tool with other ethical hacking tools to create a suite of tools that can comprehensively assess the security of an organization's infrastructure.

5. Develop a mobile version of the tool that can test the security of mobile devices and applications.

6. Expand the tool's capabilities to include testing of Internet of Things (IoT) devices, which are becoming increasingly prevalent in modern infrastructure.

Conclusion:

This focused on how we can use Ducky Script and burn the program on AT tiny85 chip using Arduino IDE.

In this paper we demonstrated the process of writing a malware payload which can exploit Windows vulnerability to launch an attack on a victim's machine. The payload can be executed from the victim's machine or remotely. Our aim in this project was to launch the attack remotely targeting a Windows machine. To create the malware and launch the attack.

References:

[1] Kumar, S. S., & Venkatesan, S. (2021). Using USB Rubber Ducky to exploit target computers. Journal of Ambient Intelligence and Humanized Computing, 12(4), 3365-3374.

[2] Trivedi, S., & Joshi, R. (2019). Hacking with a $2 microcontroller: The Digispark Attiny85. International Journal of Advanced Research in Computer Science, 10(2), 413-418.

[3] Kumar, V. R., & Shidhaye, S. S. (2020). Using Digispark ATtiny85 as rubber ducky for exploiting windows operating system. International Journal of Engineering Research and Technology, 9(11), 193-197.

[4] Almutairi, A. (2018). The USB rubber ducky and Arduino microcontrollers: Tools for ethical hackers. International Journal of Cyber-Security and Digital Forensics, 7(3), 57-64.

[5] Das, A., & Saha, S. K. (2021). Digispark Attiny85 based USB Rubber Ducky Attack. International Journal of Computer Science and Information Security, 19(5), 36-41.