BEYOND THE FIREWALL TO DEMYSTIFYING OFFLINE DEVICE VULNERABILITIES

GUIDE NAME:

Mrs.M.Amsavani,M.Tech.
Assistant Professor,
Department of CSE

STUDENT NAME:

L.AKIL - 511920104001
A.JAGANARUL - 511920104020
V.JAYAMALAN - 511920104024

ABSTRACT

- The realm of offline device hacking, also known as offline device vulnerabilities, presents a unique challenge in the cybersecurity landscape. Unlike their online counterparts, these isolated systems lack the traditional entry points like network connections, making them incredibly resilient against conventional cyberattacks.
- We aim to investigate and demonstrate alternative techniques with the potential to bypass security measures and extract sensitive information from offline device vulnerabilities.

- We aim to investigate and demonstrate alternative techniques with the potential to bypass security measures and extract sensitive information from offline device vulnerabilities.

PROBLEM STATEMENT

- **Exploiting vulnerabilities in offline systems:**

Rubber Ducky payloads can leverage various vulnerabilities, like keyboard emulation attacks, to bypass security measures and gain unauthorized access.

- **Data exfiltration from air-gapped systems:**

Devices physically isolated from networks can still be compromised through Rubber Ducky payloads that steal sensitive information stored locally.

- **Physical access requirement:**

Unlike remote hacking methods, Rubber Ducky attacks necessitate physical access to the target device, making them more targeted but also potentially easier to detect.

LITERATURE SURVEY

Title	Author & Year	Content
Supply chain vulnerabilities	Christopher Hochstein (1998)	This present a critical attack vector, necessitating secure manufacturing practices and rigorous component verification procedures.
Side-channel attacks	Paul Kocher (1996)	This remain a potent threat to air-gapped systems, with advancements in EME analysis and timing attacks posing significant challenges.
Improved Hardware hacking techniques	Steven Levy (1975)	These are becoming increasingly sophisticated, requiring robust physical security measures and tamper-proof designs.

EXISTING SYSTEM

- **Existing System Vulnerabilities:**

Legacy operating systems: Older operating systems, like Windows XP or certain Linux distributions, might have unpatched vulnerabilities exploitable through Rubber Ducky keystroke emulation attacks.

Human error: Social engineering tactics often combined with Rubber Ducky attacks can trick users into plugging the device into their system, granting attackers access.

- **Existing System Problem Statements:**

Limited awareness and training: Organizations might not be adequately aware of Rubber Ducky threats or lack proper training for employees to identify and avoid such attacks.

Outdated security protocols: Outdated antivirus software or lack of endpoint detection and response (EDR) tools might fail to detect and prevent Rubber Ducky payloads.

PROPOSED SYSTEM

- **Multi-layered security:**

Implementing a combination of physical access control measures, endpoint detection and response (EDR) tools, application sandboxing, and secure coding practices can create a robust defence against Rubber Ducky payloads.

- **User awareness and training:**

Educating employees about social engineering tactics and the risks associated with unauthorized USB devices can significantly reduce the chances of successful attacks.

- **Regular security audits and penetration testing:**

Proactively identifying and patching vulnerabilities through regular security assessments can minimize the attack surface for Rubber Ducky exploits.

ADVANTAGES OF PROPOSED SYSTEM

- **Focus on vulnerabilities:**

Exploring advantages often involves analyzing how to exploit vulnerabilities, which can inadvertently provide valuable information to malicious actors seeking to exploit those same vulnerabilities.

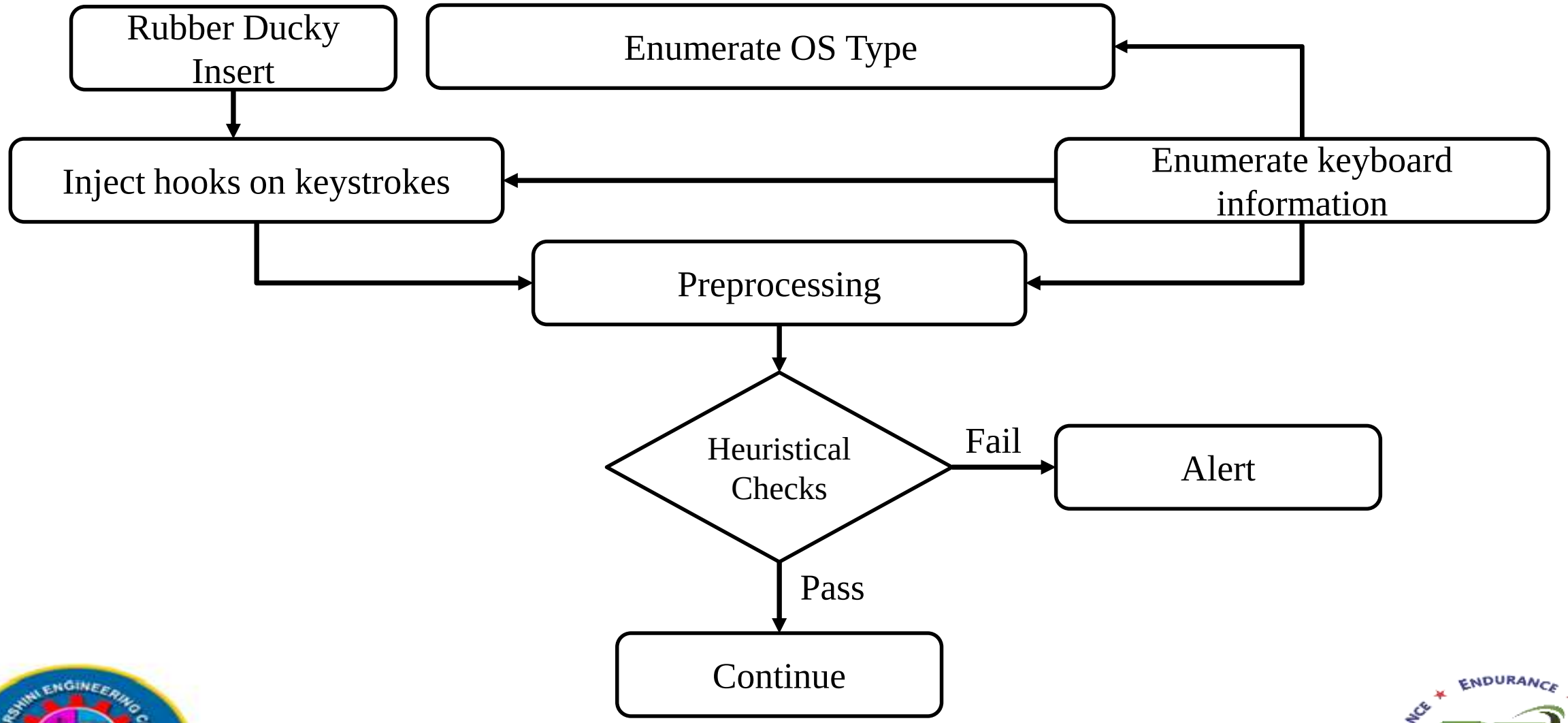
- **Ethical considerations:**

Focusing on advantages of offensive tools can overshadow the significant ethical concerns surrounding their potential misuse, potentially harming individuals and organizations.

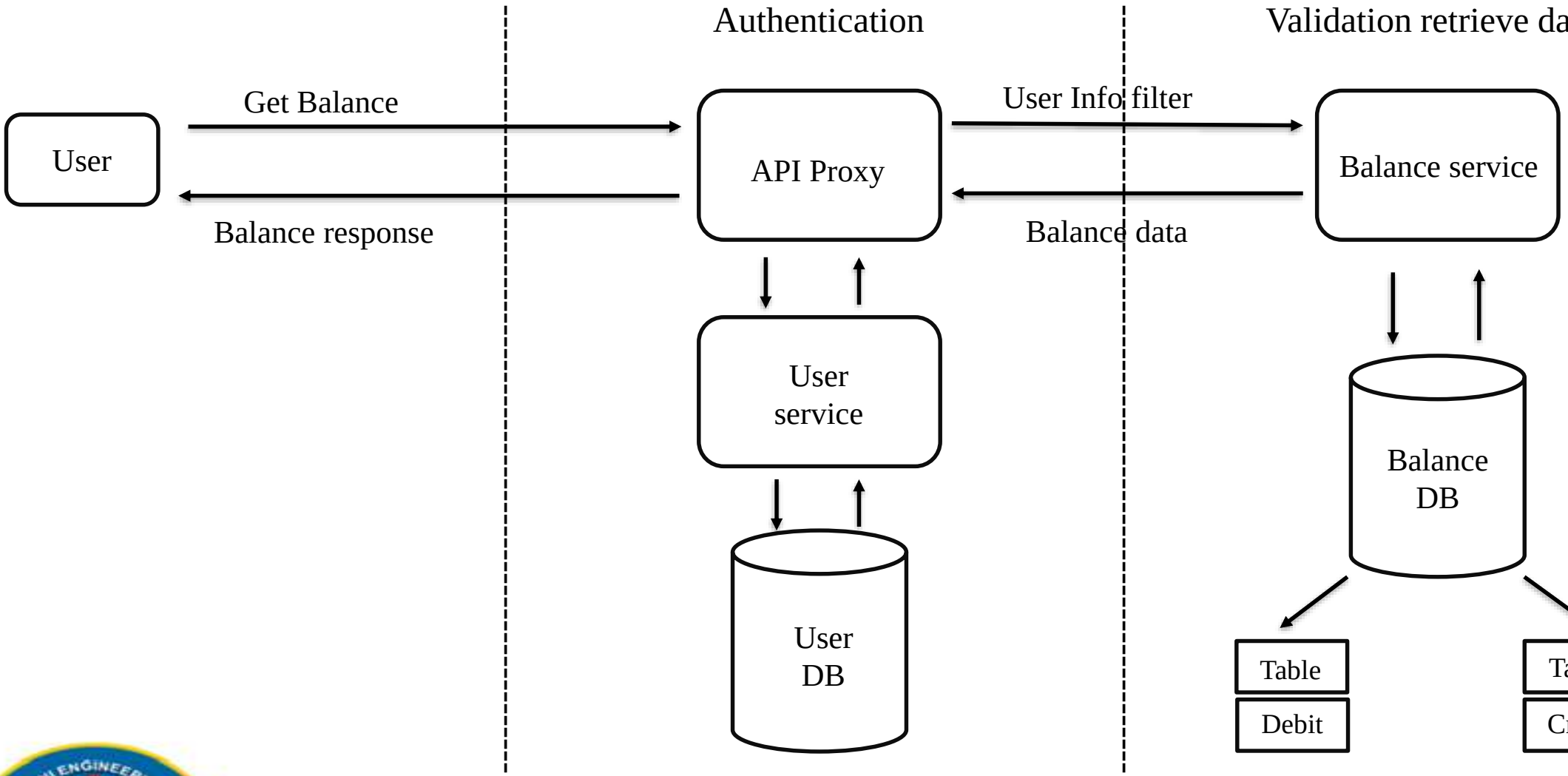
- **Limited scope:**

Examining only advantages presents an incomplete picture, neglecting the broader negative consequences and potential risks associated with such tools.

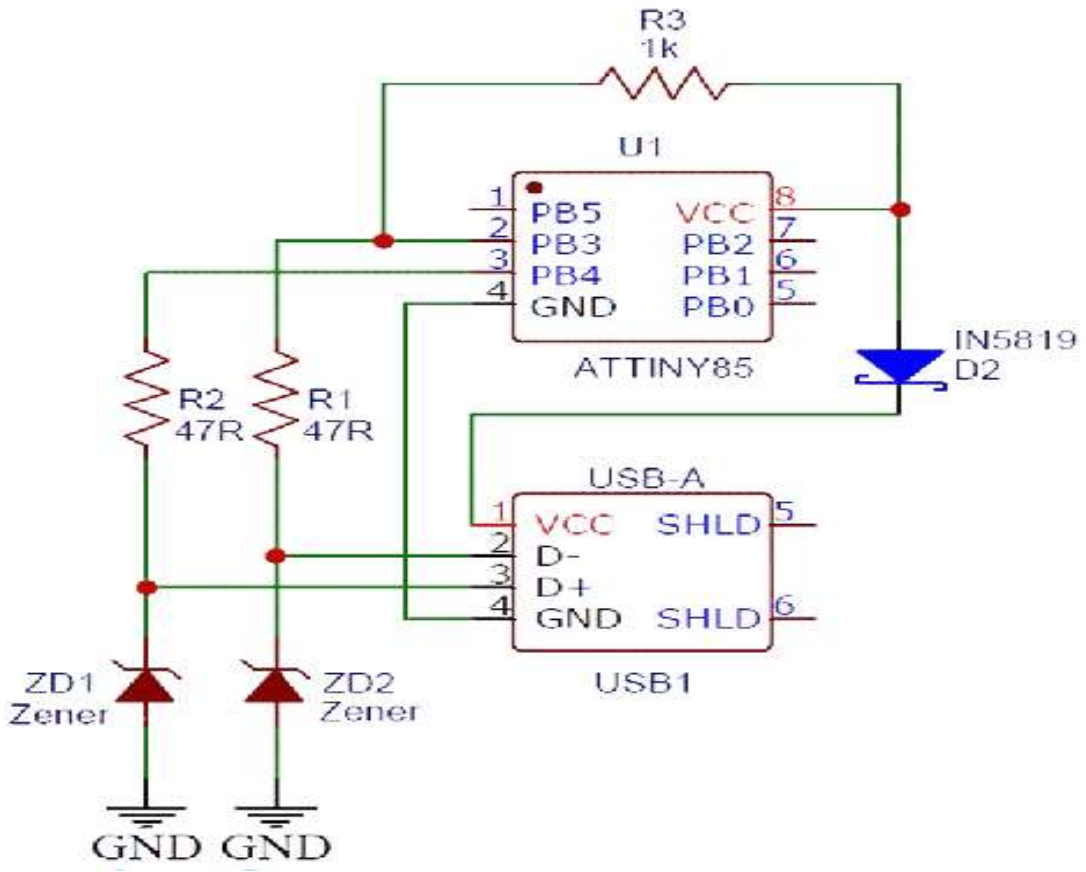
ARCHITECTURE DIAGRAM



FLOW DIAGRAM



PIN DIAGRAM



RUBBER DUCKEY

REQUIREMENTS

- **Software Requirements:**
  Scripting language
  Payload development
  Payload storage and transfer
  Arduino IDE
- **Hardware Requirements:**
  Microcontroller
  E - Devices
  USB ATTiny85 Rubber Ducky
  Multi-Audio Port

MODULES

- **ETHICAL IMPLICATION:**

1.Ethical hacking requires consent and controlled environments:

Ethical security professionals only use hacking tools and techniques with explicit permission and within controlled settings to identify and patch vulnerabilities. Rubber Ducky misuse.

2.Can have serious consequences:

Using Rubber Ducky for unauthorized access to systems can be illegal and lead to significant legal repercussions. Additionally, it can compromise sensitive data and harm individuals or organizations.

MODULES

- **ALTERNATIVE AND ETHICAL WAYS:**

3.Online courses and resources:

Numerous platforms offer comprehensive online courses and resources on cybersecurity concepts, penetration testing, and ethical hacking practices.

4.Capture the Flag (CTF) competitions:

These gamified challenges provide a safe and legal environment to test your hacking skills and learn about vulnerabilities without causing harm.

5.Bug bounty programs:

Many companies offer bug bounty programs where security researchers can ethically disclose vulnerabilities and earn rewards for their findings.

PENETRATION TESTING

USB Rubber ducky is an HID device that looks similar to a USB Pen drive. It may be used to inject keystroke into a system, used to hack a system, steal victims essential and credential data can inject payload to the victim’s computers. The main important thing about USB Rubber ducky is that it cannot be detected by any Anti-Virus or Firewall as it acts as an HID device.

HID DEVICE

HID stands for **H**uman **I**nterface **D**evices, it includes devices like keyboard, mouse, joystick. which acts as an interface between the computer and human beings. That is why it cannot get detected as the computer thinks its an interface.

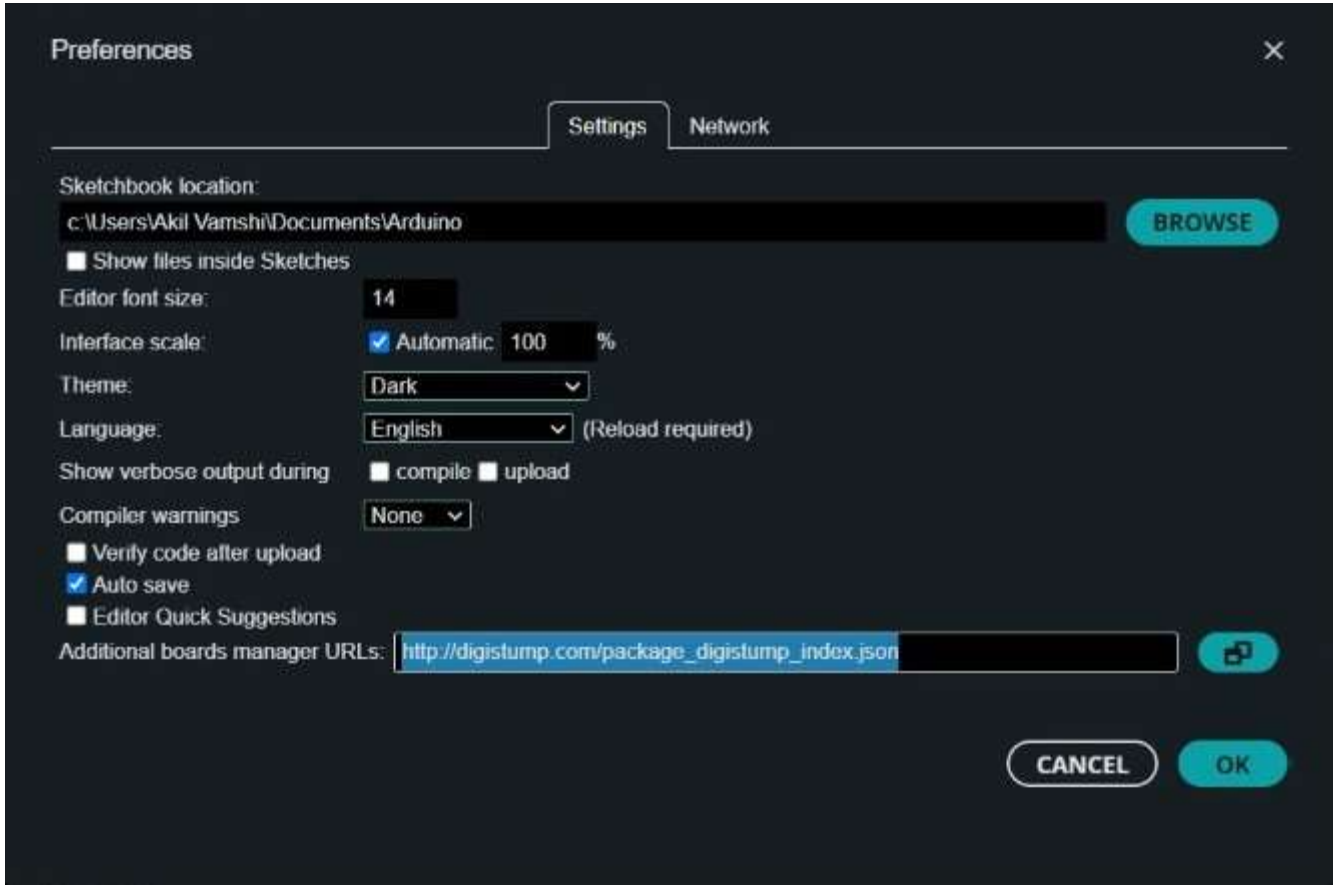
CRITERIA

- USB Rubber ducky is a kind of key injection tool, can be used as malicious or non-malicious keystroke.
- It is one of the favorite devices of hackers penetration testers as it is very fast and did not detect by ant PC.
- USB Rubber Ducky can also be used for targeting vulnerable systems or programming processes and save times.

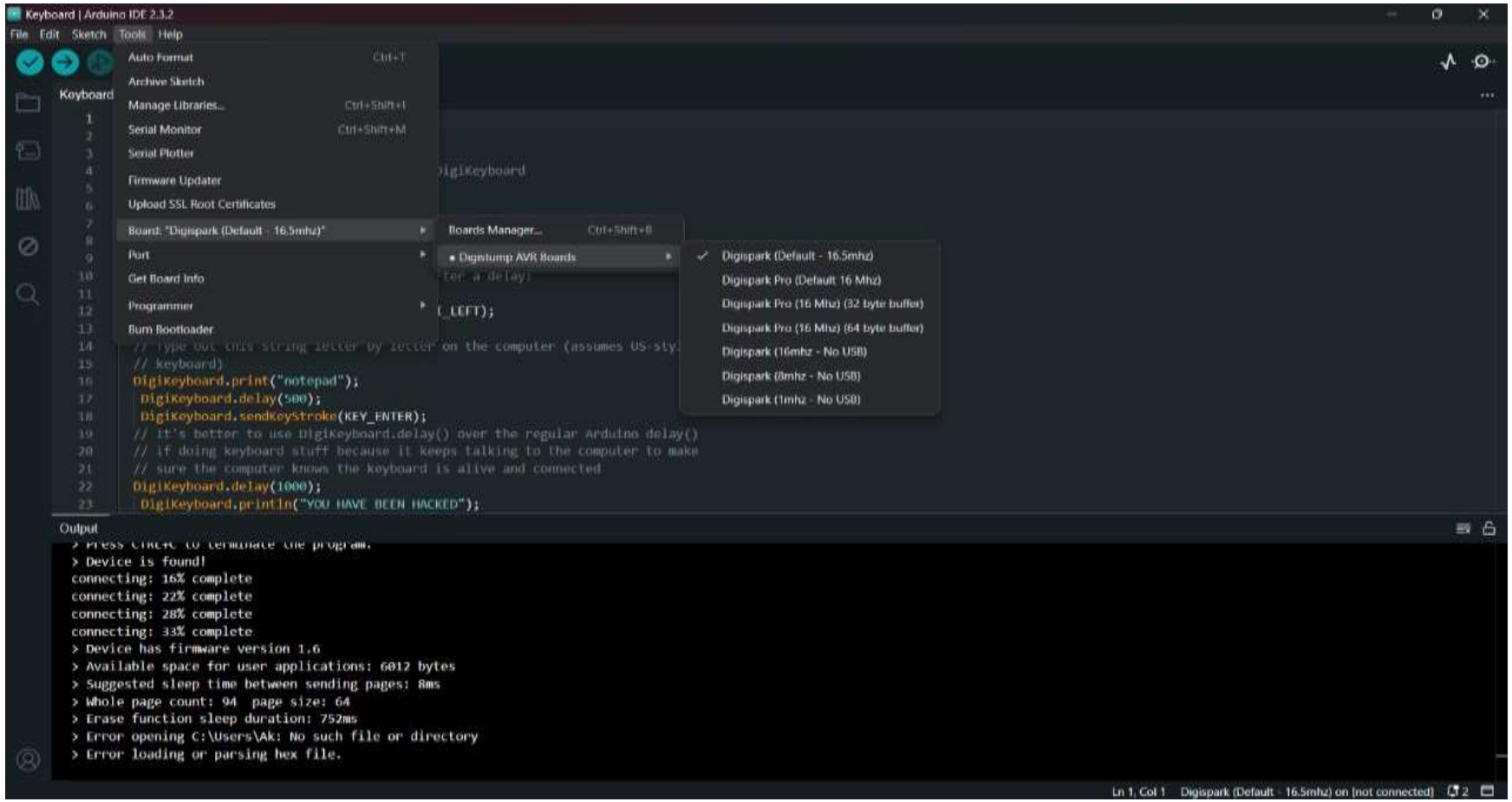
WORKING PROCESS

- USB rubber ducky acts as a keyboard and has keystrokes installed in it.
- When we connect it to PC, the keystrokes run automatically.
- It has a high speed of approx. 1000 words per minute. So those works which can be done by keyboard can also be done by USB rubber ducky.
- Whenever it is connected to a System it acts as a keyboard and executes the command which is uploaded on it.
- The commands used in this are known as payloads and written in Ducky script. One basic script is written below.

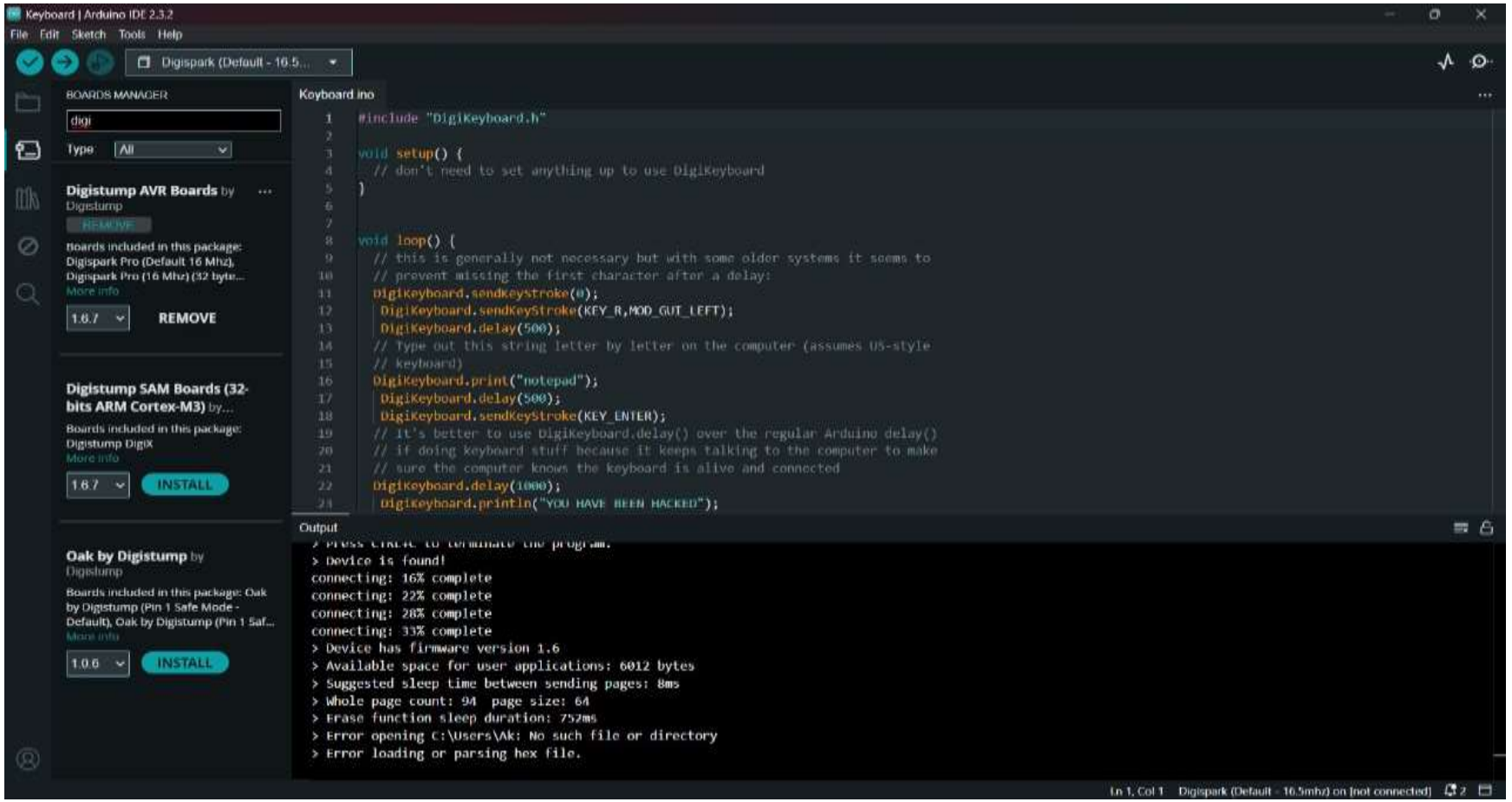
ADDITIONAL BOARD MANAGER



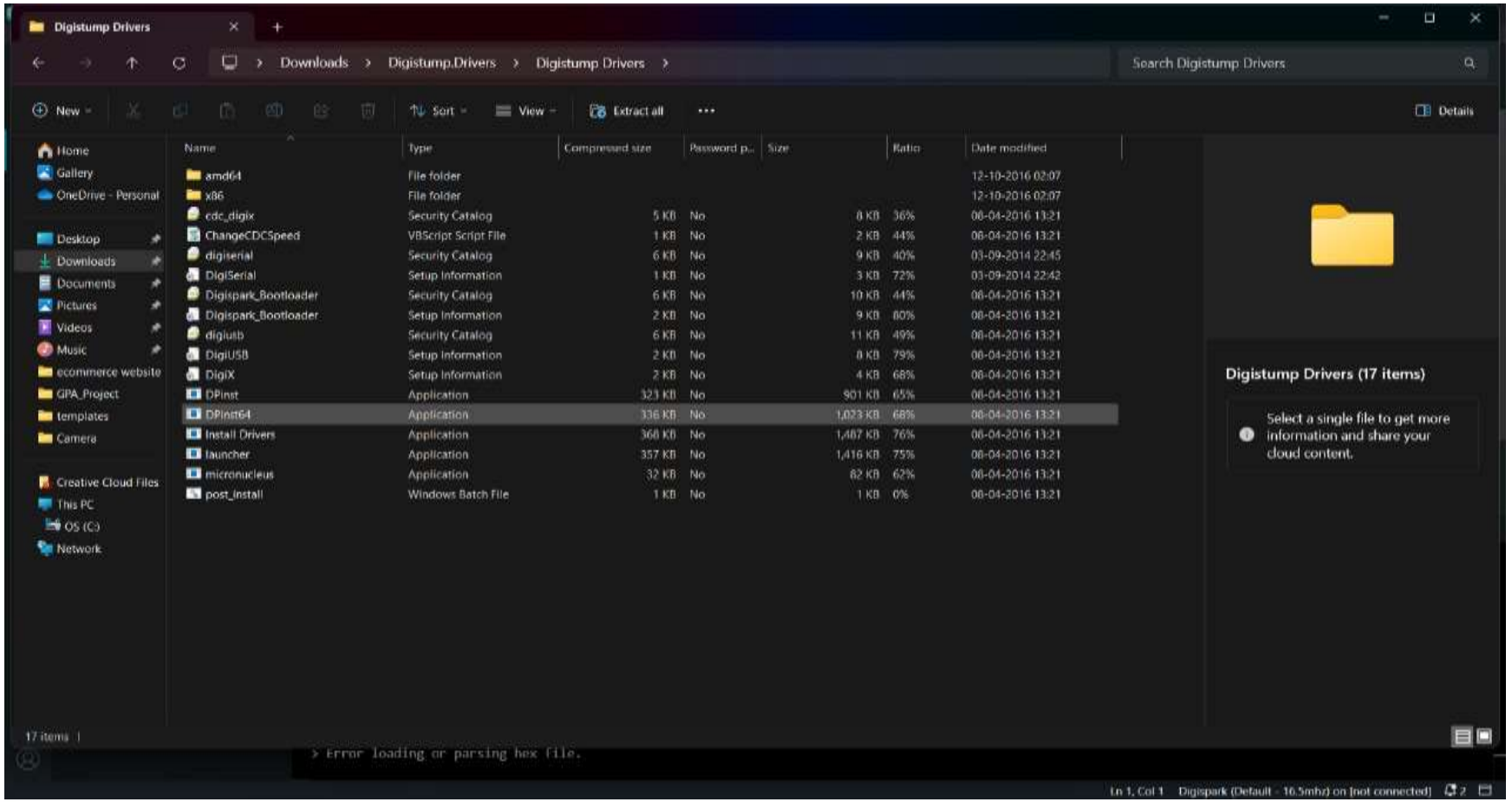
AVR BOARD SET UP



DIGISTUMP DOWNLOAD



DRIVER EXTRACT



REFERENCE

- Christopher Hochstein’s Supply chain vulnerabilities. (1998)
- Paul Kocher’s Side-channel attacks. (1996)
- Steven Levy’s Improved Hardware hacking techniques. (1975)
- D. Tian, A. Bates and K. Butler: Defending Against Malicious USB Firmware with GoodUSB. ACSAC ’15, December 07-11, 2015, Los Angeles, CA, USA.
- BlackHat USA 2014, Karsten Nohl and Jakob Lell, BadUSB - On Accessories that Turn Evil, https://srlabs.de/badusb/, Accessed on 07 Jan 2015
- S. Kamkar, USBDriveBy, http://samy.pl/usbdriveby/, Jan 2015
- Nikhil "SamratAshok" Mittal, Kautilya, https://github.com/samratashok/Kautilya, Jan 2015

CONCLUSION

The ATTiny85's small form factor, low power consumption, and keyboard emulation capabilities make it an ideal choice for projects like the Rubber Ducky. Its flexibility and affordability open up a wide range of possibilities for creative and practical applications in the realm of DIY electronics and cybersecurity. However, it's essential to use such technology responsibly and ethically, respecting privacy and security considerations.