Co-funded by the
Erasmus+ Programme
of the European Union

PROPOSAL:

Securing messages using heat

Participant #1
- **Name: Abigail Machaj**
- **Rzeszów University of Technology**
- **Country: Poland**

Participant #2
- **Name: Alicja Siekanowicz**
- **Rzeszów University of Technology**
- **Country: Poland**

1

1. Introduction **3**

2. Why use it **3**

2.1. General description of the problem 3

2.2. Cyber-attacks 3

2.3. Security during war 3

2.4. Almost impossible to crack 4

3. Where to use it **4**

4. How it all looks like **4**

4.1 Website 4

4.2 Pendrive-like device 5

4.3 Heating device 5

4.4 Heating-type program 6

4.5 Eliminate abnormalities 6

5. How it works on the outside **6**

6. How it works from within **7**

Subject/title: Securing messages using heat.

1. Introduction

In today's world, especially when the war is at the break, it is difficult to find a solution to secure the message flow. With every new method to keep the information safe, cybercriminals create more solutions to break the code. It is hard to come up with something unhackable. We want to introduce an idea of our concept for encrypting messages using heat. Such idea can have a significant impact on the future safety of the military as well as civil facilities. Our purpose is to keep the message flow in check, protecting society from injustice they don't deserve. There will always be problems with the security system, but we will do our best to make it safe as long as we can.

2. Why use it

2.1. General description of the problem

The usage of our method has also non-military benefits. From the economic point of view, if idea is well received we can think about making a few changes and using it in banks' security systems or even other as important facilities. The modern world is threatened by many cyber-attacks which make people more scared about their well-being, especially when most of their money is stored online. A lot of young people live their lives online, with the whole of their memories placed on social media or even google drive where most of them have important documents and photos. We believe that this method could be safer compared to how it works now. With that in mind, it is also important to add a safer flow of messages in the military can also lower the risk of attacks on field hospitals or shelters for soldiers and civilians. Ethically thanks to at least fewer losses of lives, the war can be a little more humane.

2.2. Cyber-attacks

Today's world is exposed to many dangers. Cyber-attacks are the most common among them. It is estimated that one occurs every 39 seconds which in a day gives us around 202 176 000 attacks per day.

2.3. Security during war

Securing the flow of messages and other significant data is especially necessary during war. At a time like this military and other military-related establishments are exposed to the information outflow which can have a dreadful effect on the course of the war. With huge responsibility comes even greater risk. We believe that this method can be almost unbreakable without the use of our device and even then the one who stole it would need to know too many mechanics to properly operate it.

2.4. Almost impossible to crack

Hypothetically let's assume that someone stole our device and is trying to use it. Even knowing the mechanic behind it and using the device will not give him much. The change of what needs to be done is too quick for a normal person without constant intel. It does not matter if it is used by the military or corporations. The use of our device can be adjusted according to the needs.

3. Where to use it

The most prominent place for our device to be used is during important military-related actions. While training, sending secret messages or during the actual war. Many companies can benefit from this method too. A great example being banks, where security od data is a top priority. Thanks to the uncommon encryption-switching method those messages will be a challenge to intercept. Our idea strongly relies on two layers: first is a number of different encryption programs and second - the temperature of the device. Even large scale or precise attacks will have to face previously mentioned security measures and most likely will be stopped by them. Due to originality a great amount of effort and time will be needed to break the protection guaranteed by us.
Undeniably Our device is going to be a great security option to those that do not have to fear large scale attacks performed by government founded specialists. Corporations will benefit from our services once again thanks to the atypical encryption switching method. most likely Many attacks are going to be performed by people with limited resources and little experience. Our security measures are going to render such attempts futile.

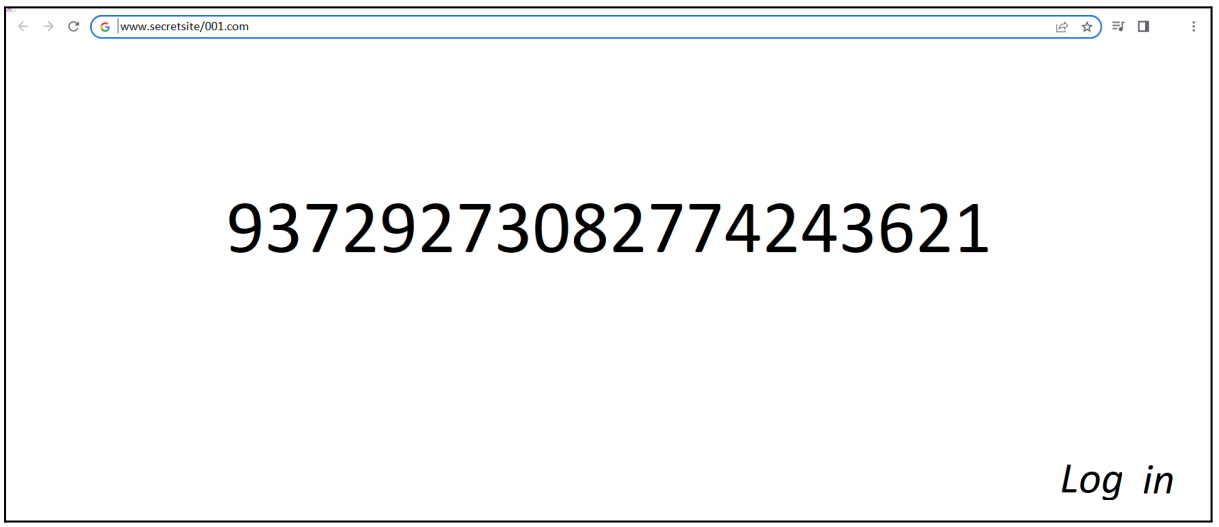
4. How it all looks like

To create our idea we will need a few devices that will cooperate with each other.

4.1 Website

- it will show some numbers (randomly generated)
- it will be a place to put secret data (after decoding the side)
- Schema:

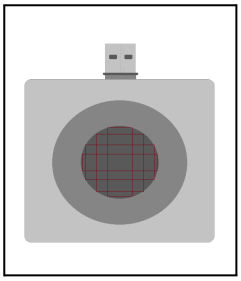
Before breaking the code:



Afterwards it will look like a notebook.

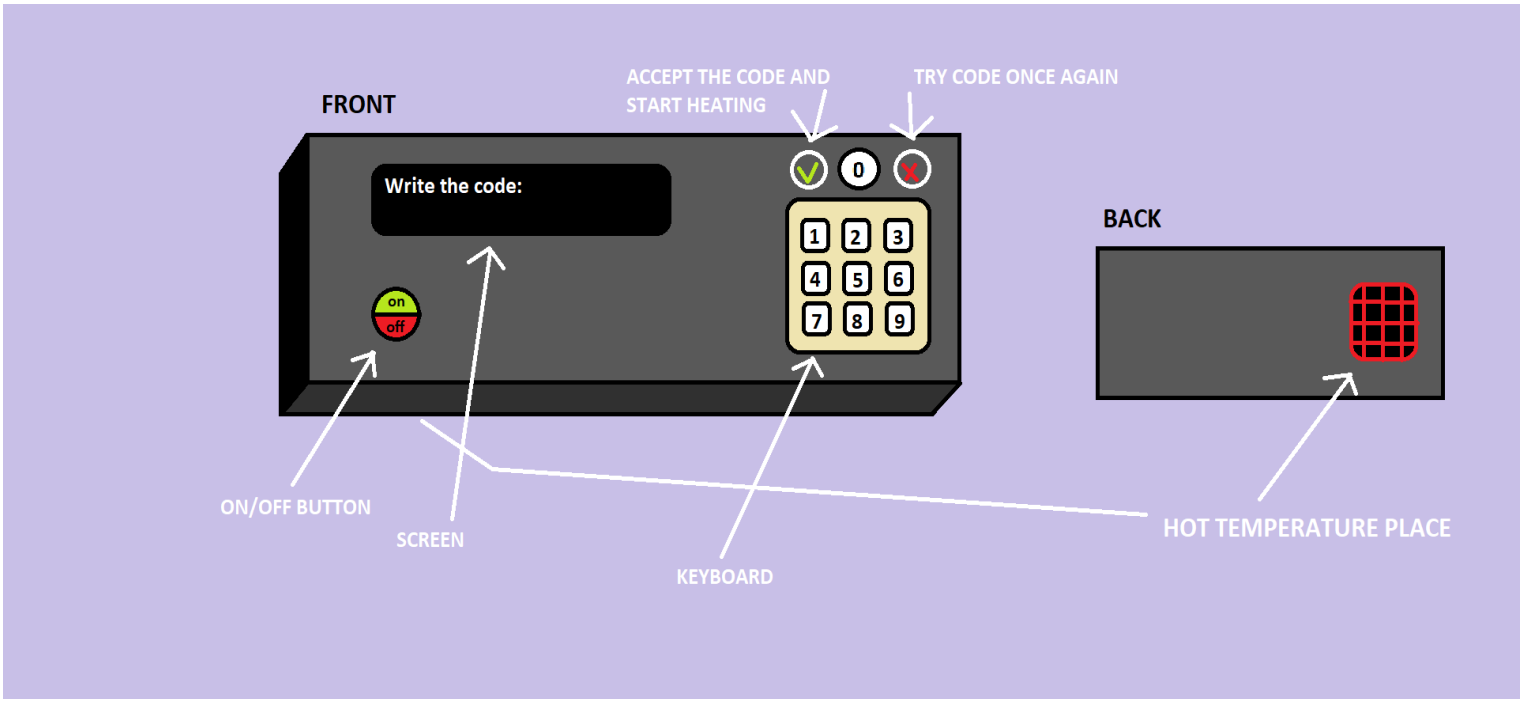
4.2 Pendrive-like device

- Function:
  - to put in the computer like a pendrive,
  - it will detect the temperature on it with an accuracy of 0,1°C between 35 and 95°C,
  - it will give the information about the temperature to the computer,
- How does it looks like:



4.3 Heating device

- After manually rewriting the numbers from the website, the device will heat its heating part to the temperature that will be needed to unlock the site.



4.4 Heating-type program

- it will transform data from pendrive-like device to unlock the protection mechanic of the website,

4.5 Eliminate abnormalities

- If the temperature taken from a pendrive-like device is not correct three times in a row, the website will be blocked on that concrete computer.

5. How it works on the outside

We came up with an idea which will use heat as a protection for the internet system. We want to create a new form of lock that will be much harder to hack. Theoretically speaking, the hacker would need to have really specific tools to hack something that is not common in general that couldn't be hacked remotely.

The website will show randomly generated numbers in a randomly generated amount (between ten and twenty). A small portable device not connected to any network will also be used, which uses the same algorithm as a website. You will have to manually enter the appropriate data displayed on the page into the device. It will process the data based on an algorithm and heat it up to the temperature indicated in the system. You will connect a temperature sensor to the computer, on which you will put a device that is also a heater. After heating the device to the required temperature, the heater screen will show the message of reaching the temperature. On the computer screen, you will need to click "log in" and the sensor will read the temperature from the heater. In this way, only an authorized person (knowing how to properly rewrite the digits to the device and the temperature-related mechanism) with the appropriate device (knowing the algorithm and generating heat based on it) is able to log into the system.

6. How it works from within

Our idea is based on the use of heat as an access key to the internet system. We want to improve today's systems with the new method of coding and decoding secret data. The website will be programmed to generate and show the numbers. The heater will have the same inside program as the site to change that number into temperature. The small device will generate heat based on that program. After putting the heater on the pendrive-like device it will be transformed into a different type of value as an access key. So the website and the heater will use the same algorithm but the first will be used to access the site and the second one will be used to generate that access key.

ASSETs+
Alliance for Strategic Skills addressing Emerging Technologies in Defence

Co-funded by the Erasmus+ Programme of the European Union

III EDITION
2022-2023

AALBORG UNIVERSITY · AEROCAMPUS AQUITAINE · ANDALUCÍA AEROSPACE · AIRBUS · CenSec · CentraleSupélec · CIMEA · DAC · EWF · FADA

GICAN · Fondazione Giacomo Brodolini · HENSOLDT · LEONARDO · LEONARDO · Mercantec · Navantia · POLITECHNIKA RZESZOWSKA · RMA Royal Military Academy · ROLLS ROYCE

SEA Europe · SAAB · SAFRAN · UCA Universidad de Cádiz · uc3m Universidad Carlos III de Madrid · université de BORDEAUX · POLITÉCNICA · UNIVERSIDAD DE SEVILLA · SCUOLA SUPERIORE SANT'ANNA 1345 UNIVERSITÀ DI PISA

ASSOCIATED PARTNERS: eupportunity · reportbrain

@ASSETS_Plus · @ASSETs+ · ASSETs_Plus_EU | www.assets-plus.eu