https://www.google.com/a/cpanel/guttman.ort.org.il/images/logo.gif?service=google_default

**מערכת גישה אוטומטית לאתרים**

**מבוססת SSO**

*תיק פרויקט*

***אליזבת לנגרמן***

ת.ז: 208568675

בית ספר: אורט גוטמן נתניה

מורים מנחים: מיכאל צ'רנובילסקי

גד רוזנטל

תאריך הגשה: 04.2016

**תוכן עניינים**

מבוא ורקע לפרויקט.................................................................................... 3

המטרות המרכזיות..................................................................................... 4

דרישות המערכת..................................................................................... 4

תיאור המוצר............................................................................................. 5

סביבת העבודה......................................................................................... 8

ארכיטקטורת המערכת................................................................................ 9

פירוט מבני הנתונים.................................................................................... 26

פירוט מאגרי המידע (ומסד הנתונים)............................................................. 27

מדריך התקנת המערכת.............................................................................. 31

ממשק המשתמש....................................................................................... 32

תהליך מחקר ופיתוח.................................................................................. 35

בבליוגרפיה............................................................................................... 37

קוד הפרויקט............................................................................................. 38

**מבוא ורקע לפרויקט**

כולנו רשומים כיום למספר רב של אתרים שנותנים לנו שירותים שונים. לדוגמא: כתובת אימייל אחת או יותר, גישה לחשבון הבנק שלנו דרך האינטרנט, קניות אונליין בחנויות שונות, חשבון פייסבוק, ושירותים רבים נוספים שמאפשרים להירשם אליהם כמנוי באמצעות שם משתמש וסיסמא.

קל מאוד לשכוח שמות משתמש וסיסמאות כאשר אנחנו בוחרים עבור כל שירות צירופים אחרים. עם זאת, כדי לשמור על הפרטיות שלנו ולהקטין את הסיכונים, אנחנו מעדיפים לא להשתמש באותה סיסמא, אלא להחליף אותה בכל אתר. לרוע המזל, כך קל מאוד לשכוח את אחת הסיסמאות או להתבלבל ביניהן. בנוסף, עלולה להיות אפשרות של Phishing. כלומר, אתרים מדומים שמתחקים אחר אתרי אינטרנט מוכרים, ומפנים את המשתמש לאתרים מזוייפים. כך הם עלולים לגנוב סיסמאות ומידע פרטי של המשתמשים.

הפרויקט שאני מפתחת מטרתו לתת מענה לבעיה זו, ע"י בניית מערכת הפועלת בשיטת SSO (Single Sign On). זוהי שיטת הזדהות של משתמש המאפשרת הזדהות אחת כלפי מספר מערכות מידע, ללא צורך בהזדהות נפרדת עבור כל מערכת.

המוצר שאני מפתחת אמור לתת למשתמש מסויים אפשרות גישה לאתרים שונים ללא צורך בסיסמאות רבות. המשתמש יוכל להתחבר למערכת (באמצעות סיסמא אחת בלבד) והיא תאפשר לו להתחבר לשירותים שתומכים במוצר זה ללא צורך בשם משתמש וסיסמא ייחודיים. כלומר, במקום להתחבר כרגיל, המשתמש יבחר באופציה המתאימה ויקבל גישה לחשבון שלו באופן אוטומטי.

**המטרות המרכזיות**

המטרות המרכזיות של הפרויקט שאני מפתחת הן:

* לאפשר גישה ישירה, מהירה ואוטומטית לאתרי אינטרנט שתומכים באפשרות זו.
  + הגישה תהיה באמצעות התחברות אחת בלבד, שתאפשר למשתמש להתחבר לחשבון שלו במספר אתרים ללא צורך באמצעי זיהוי רבים.
* להפוך את השימוש בסיסמאות לקל ונוח יותר.
  + להקל על המשתמש שלא יצטרך לזכור סיסמאות רבות ושונות.
  + ישנן פניות רבות של משתמשים שנושא סיסמאות ושחזורן. לכן מערכת כזו יכולה לצמצם עלויות של צוותי מחשוב שמטפלים בפניות אלה.
* להגדיל את האבטחה ע"י הקטנת הסיכוי לגניבת סיסמאות באמצעות PHISHING (אתרים מדומים).

**דרישות המערכת**

דרישות פונקציונאליות:

* לאפשר התחברות לתוכנית הראשית, באמצעות שם משתמש וסיסמא.
* לאפשר למשתמש שהתחבר גישה לתוכניות משניות התומכות באפשרות זו, ללא צורך בשם משתמש וסיסמא.
* להציג למשתמש המחובר את האתרים שבאפשרותו להתחבר אליהם באמצעות מערכת זו.
* לתת למשתמש אפשרות להתנתק מהמערכת.
* אפשרות חיבור של מספר משתמשים בו זמנית (multi-client).

דרישות ממשקים:

* כל אחת מהתוכניות (ראשית ומשנית) תכיל ממשק גרפי עבור המשתמש (GUI).
* תקשורת בין התוכנית הראשית לתוכניות המשניות שיאפשר התחברות.
* תקשורת בין השרת הראשי ללקוחות המתחברים אליו באמצעות אינטרנט.

דרישות לא פונקציונאליות:

* אבטחה: שמירה מאובטחת על סיסמאות והעברה מוצפנת של מידע.
* אפשרות צפייה בסטטוס המשתמשים לצרכי תחזוקה.

דרישות מסד נתונים:

* שמות המשתמש והסיסמאות לתוכנית הראשית יישמרו בDatabase של 3SQLITE.

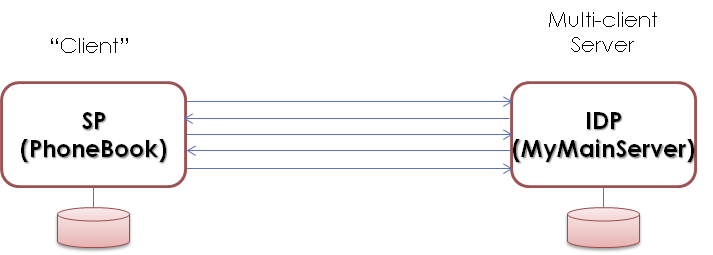
**תיאור המוצר**

המערכת שאני בונה מורכבת משרת מרכזי, "השרת הראשי" שכיניתי MyMainServer, וכן משרת נוסף לדוגמא, "שרת משני" (SP). השרת הראשי מספק את שירות ה- SSO שאני מעוניינת לבנות במערכת שלי, ואליו השרת המשני מדמה אתר אינטרנט כלשהו שאליו מתחברים משתמשים רשומים, והוא משתמש בשירות שאני מציעה.

תהליך התחברות משתמש למערכת מתבצע כך:

ראשית, שרת שמעוניין ליצור קשר עם המערכת, מתחבר לשרת הראשי באמצעות socket. במסגרת התקשורת ביניהם (client-server), מקבל השרת המשני (ה- SP) מזהה ייחודי ומפתח ייחודי שדרכו תתבצע הצפנת התקשורת בינו לבין השרת הראשי. הנתונים מוצפנים בעזרת הצפנה א-סימטרית, RSA. כמו כן, הוא שולח אל השרת הראשי את כתובתו, על מנת שבהמשך יוכל להפנות משתמשים בחזרה אליו (באמצעות redirect).

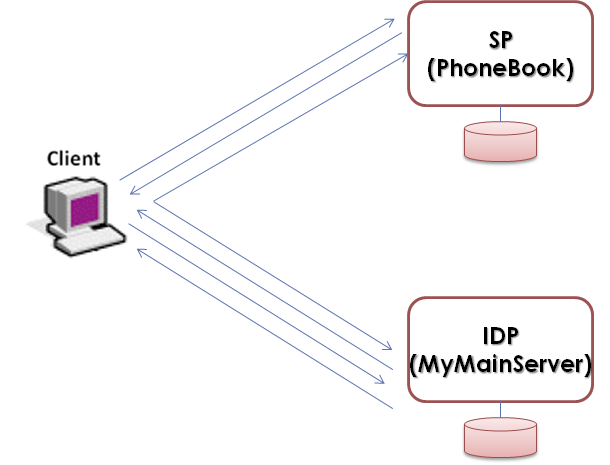
לאחר חילופי המידע, השרת החדש נרשם במסד הנתונים של השרת הראשי.



כעת, משתמש שמבקש להתחבר לשרת ה-SP (לדוגמא, השרת PhoneBook), יכול לבחור באופציה המתאימה ולהתחבר באמצעות MyMainServer, השרת הראשי.

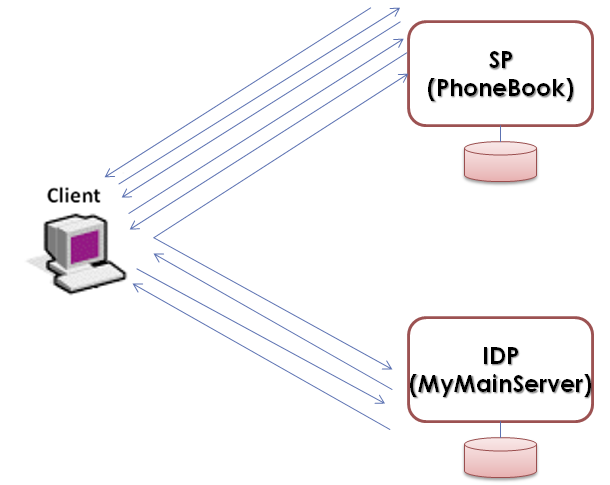
בבחירת האופציה, המשתמש יועבר (ע"י redirect) לשרת הראשי, ויבצע מולו את ההתחברות עם שם משתמש וסיסמא. חשוב לציין ששם המשתמש והסיסמא משמשים רק לשם התחברות ל-MyMainServer ולא לשרת של אתר האינטרנט שהמשתמש ביקש להתחבר אליו מלכתחילה.

השרת הראשי ימצא את המשתמש במסד הנתונים, ויעביר את ה- ID שלו כפי שהוא רשום בשרת ה-SP. הוא יפנה את המשתמש בחזרה אל השרת המשני, אל העמוד השייך לו, העמוד שמכיל את הפרטים של משתמש זה.



באם משתמש חדש רוצה להירשם לאתר המשתמש במערכת, הוא נכנס כרגיל להרשמה של אותו אתר. המשתמש מופנה אל דף ההרשמה של השרת הראשי, ונרשם אליו באמצעות שם משתמש וסיסמא. לאחר שנוסף את מסד הנתונים של השרת הראשי, מופנה המשתמש שוב אל השרת המשני, אל דף ההרשמה שלו. בדף זה יוכל להכניס נתונים שונים כדי להשלים את הרשמתו לאתר שביקש להירשם אליו.

במילים אחרות, יבצע את כל ההרשמה כמו שהיא מול שרת ה- SP, אך כל הטיפול בהתחברות ובסיסמאות יישאר בידי השרת הראשי, MyMainServer.



**סביבת העבודה**

הפרויקט נכתב ב Python 2.7, בסביבת העבודה Pטא

**ארכיטקטורת המערכת**

הפרויקט מורכב משני שרתים מרכזיים: השרת הראשי ()IDP, ושרת לדוגמא שיתמוך באפשרות שאני מפתחת (SP). בשני השרתים תהיה תמיכה לחיבור לקוחות במקביל- multithreading.

*השרת הראשי(IDP) - חלוקה למודולים:*

* **New User Registration**

מודול שאחראי על הרשמה של משתמשים חדשים, בין אם לשרת SP מסויים או לשרת המרכזי- IDP בעצמו.

* מקבל מזהה של הSP שממנו נשלחה הבקשה
* מקבל ID של המשתמש כפי שנרשם בשרת ה SP ושומר אותו
* מבקש פרטי הרשמה או התחברות מהמשתמש
* בודק האם המשתמש קיים, או שהוא חדש לחלוטין
* בהתאם, שומר את המידע החדש שנוסף על משתמש זה
* Redirect בחזרה לשרת הראשון (SP) + הודעת הצלחה
* **User Login**

מודול שתפקידו לאפשר למשתמש להתחבר לשרת הראשי ומספק את פרטי ההתחברות של המשתמש לSP.

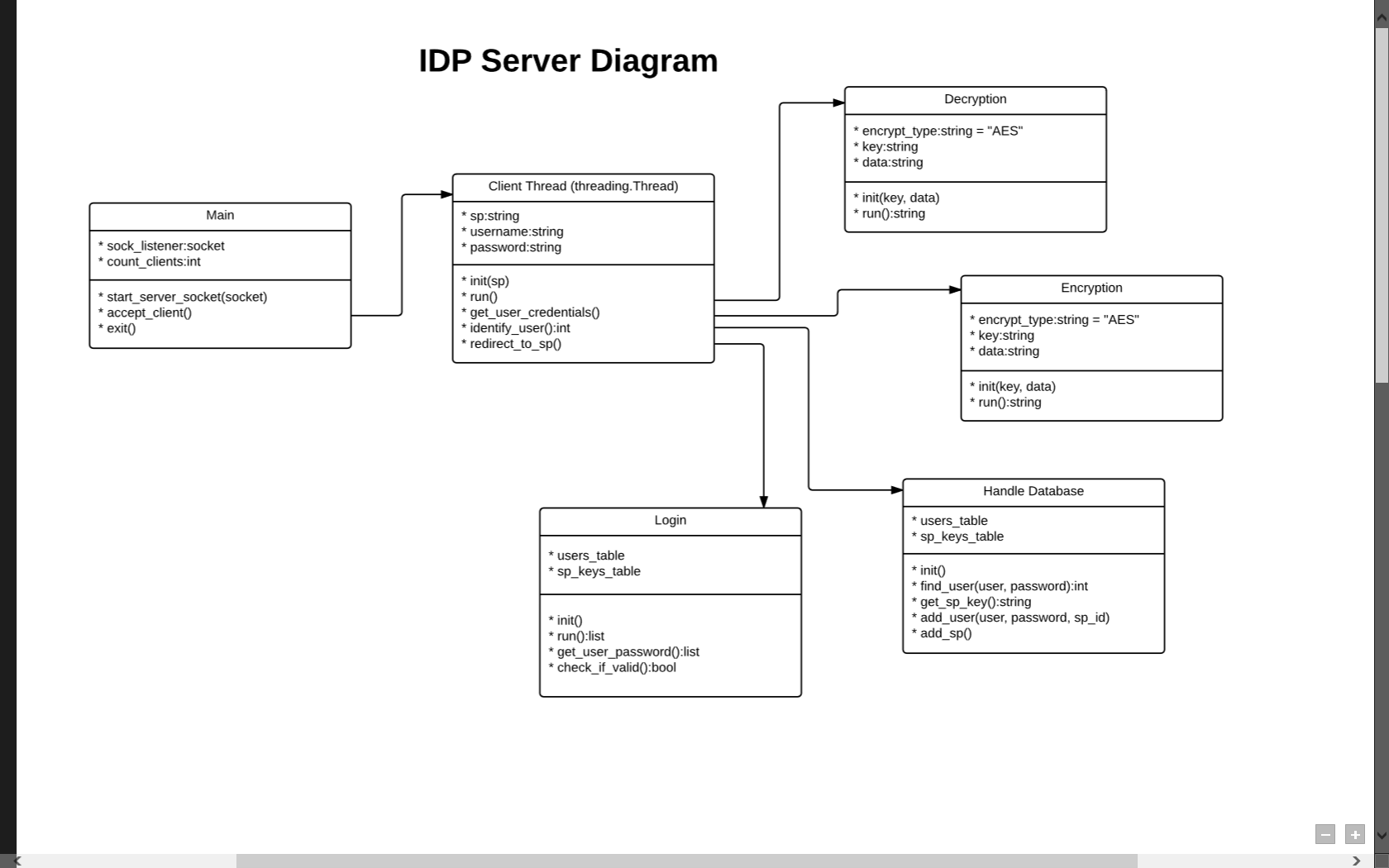
* מקבל מזהה של הSP שממנו נשלחה הבקשה לזיהוי לקוח
* מבקש מהמשתמש להכניס פרטי זיהוי
* מוודא את קיום המשתמש (בהתאם לDatabase)
* ממפה בין המשתמש לבין ה ID שלו בשרת ה SP המבקש
* Redirect בחזרה לשרת הראשון (SP) + שליחת user SP ID ל SP.
* **SP Registration**

מודול שתפקידו תקשורת ראשונית עם שרת שמתחיל להשתמש במערכת.

* מקבל בקשה משרת הSP החדש
* מבקש ממנו פרטים חיוניים לתקשורת ביניהם (לדוגמא מידע כללי, הכתובת שאליה לעשות redirect, רשימת מזהים של המשתמשים הרשומים לשרת זה)
* מנפיק מפתח להצפנה סימטרית בין שני הצדדים ושולח לSP.
* **Handle Database**

המודול מכיל את מסד הנתונים ואת הכלים לעבודה מול מסד הנתונים.

* אפשרות הוספת משתמש
* חיפוש משתמש והחזרת ה ID שלו בהתאם לSP המבקש
* חיפוש SP ואפשרות להוספה



*השרת המשתמש במערכת(SP) - חלוקה למודולים:*

* **Login**

מודול המאפשר למשתמש כלשהו להתחבר לשרת.

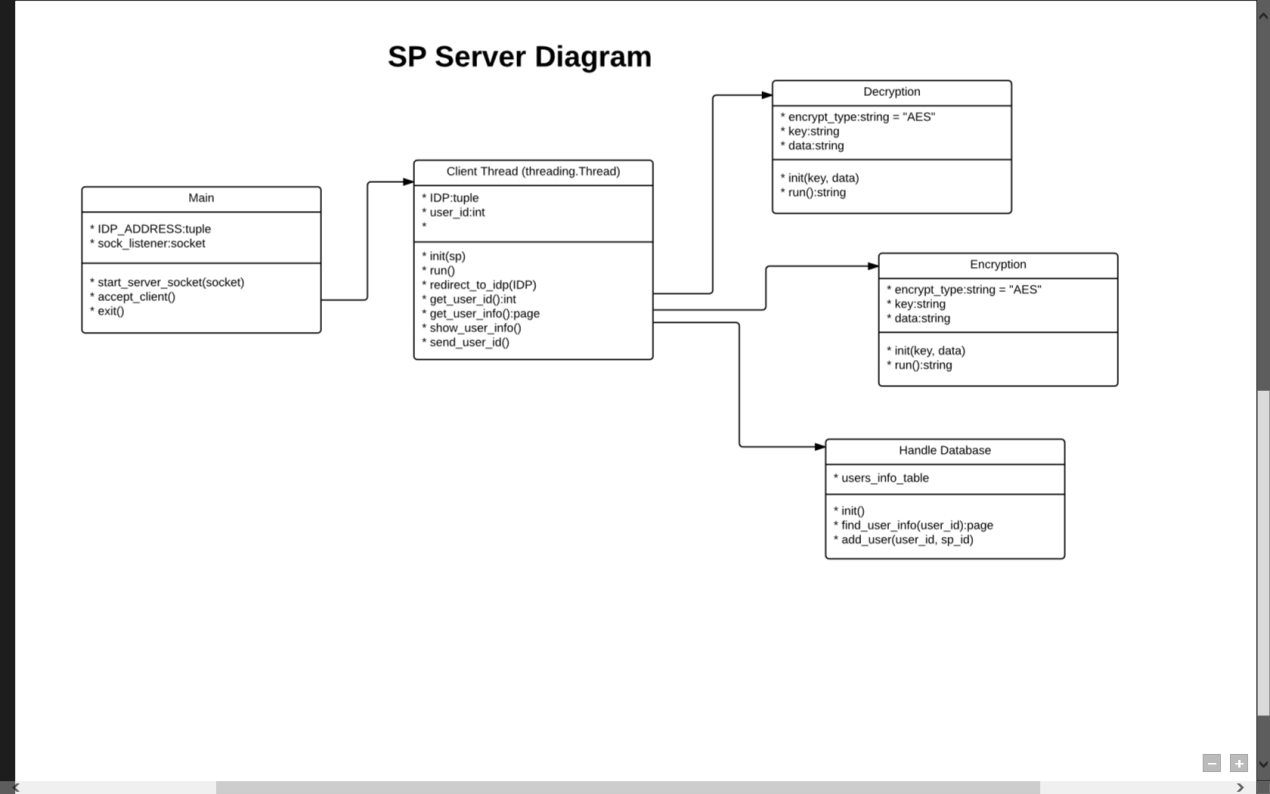
* אפשרות התחברות באמצעות שם משתמש וסיסמא או באמצעות שרת ה IDP.
* Redirect לשרת המרכזי IDP + שליחת מזהה ייחודי מוצפן של הSP.
* הצגת נתוני המשתמש אחרי ההתחברות, כרגיל.
* **Register**

מודול שאחראי על הרשמת משתמש חדש לאתר, והתקשורת עם השרת הראשי במצב זה.

* Decrypt
* Decode
* במקרה של הצלחה, Redirect למודול User Page
* **Handle Database**

המודול מכיל את מסד הנתונים ואת הכלים לעבודה מול מסד הנתונים.

* אפשרות הוספת משתמש
* חיפוש משתמש והחזרת העמוד הפרטי שלו בהתאם ל userID



**פירוט מבני הנתונים**

|  |  |  |  |
| --- | --- | --- | --- |
| **המודול** | **מבני הנתונים** | **סוגם** | **תפקידם** |
| MyMainServerWEB.py | self.process\_attrs | רשימה של strings | מגדיר את התכונות של תהליך שלגביהן תיתן מידע מחלקת ProcessStats |
| this\_proc\_dict | מילון string-int/string | מילון שהמפתחות שלו הם שמות התכונות של התהליך, והערכים הם הערכים של תכונות אלה בתהליך הספציפי |
| proc\_results\_list | רשימה של מילונים | רשימת כל המילונים this\_proc\_dict עבור כל התהליכים במחשב |
| MySPWEB.py | all\_process\_stats | רשימה של מילונים | רשימה שמכילה את כל הנתונים של כל התהליכים במחשב שהלקוח מקבל לאחר קריאה לפונקציית GetStats() של מחלקת ProcessStats |
| DataBaseManager.py | all\_process\_stats | רשימה של מילונים | אותה רשימה כמו הנ"ל שהשרת מקבל מהלקוח |
| g\_client\_thread\_list | רשימה של אובייקטים | רשימה של כל האובייקטים ממחלקת ClientThread שיצר השרת (כלומר מעין רשימה של כל הלקוחות) |
| Encryption.py | IT\_EMAIL\_ADDRESSES | רשימה של strings | רשימה של כל כתובות המייל של התמיכה הטכנית (IT) של החברה |
| UNITS\_CONVERSION\_DICT | מילון string-int | מילון המסייע להמיר בין היחידות השונות של מידע (Bytes, KB, MB, GB) |
| RESOURCES\_MATCH | רשימה של tuples של strings | רשימה המכילה זוגות של מחרוזות ומתאימה בין שמות "רגילים" של משאבי המחשב לבין השמות שלהם כתכונות של תהליך |
| SYS\_PROCESSES | רשימה של strings | רשימה המכילה שמות של תהליכי מערכת שמהם יש להתעלם בעת ניתוח הנתונים |

**פירוט מאגרי המידע (מסד הנתונים)**

התוכנה יוצרת בצד השרת מסד נתונים אחד לכל לקוח. שם הקובץ של המסד מתקבל מהפעלת hash על הכתובת הפיזית של המחשב (שאליה נוסף prefix). במסד הנתונים יש טבלה בודדת בשם **ResourcesData** שמאחסנת את כל הנתונים הנאספים מאותו מחשב.

מבנה הטבלה הוא:

|  |  |  |
| --- | --- | --- |
| **שם העמודה** | **סוג** | **תפקיד** |
| ProcName | VARCHAR(255) | שם התהליך |
| ProcID | INT | מזהה התהליך (ID) |
| CreatingProcID | INT | מזהה התהליך של התהליך שיצר את התהליך הנוכחי |
| ElapsedTime | INT | הזמן שהתהליך רץ בשניות |
| CpuTimePercent | INT | אחוז השימוש ב- CPU |
| WorkingSetPrivate | BIGINT | השימוש בזיכרון (ב- Bytes) |
| IOBytesPersec | BIGINT | כמות ה- Bytes שנקראו או נכתבו בפעולות I/O לשנייה |
| IOOperationsPersec | BIGINT | כמות פעולות I/O לשנייה |
| Threads | INT | כמות תתי-התהליכים |
| Date | DATE | התאריך שבו נאסף המידע |
| Time | TIME | השעה שבה נאסף המידע |

**מדריך התקנת המערכת:**

**ממשק המשתמש**

**תהליך מחקר ופיתוח**

המערכת שאני בונה בפרויקט זה מטרתה יצירת אפשרות SSO. יש מספר שיטות ליצור זאת, ולאחר מחקר על SAML ועל 2OAUTH, החלטתי שהמבנה שלSAML מתאים יותר למבנה המערכת שאני רוצה לפתח.

התחלתי לחפש מודול שיסייע לי ביצירת מערכת שפועלת לפי דוגמת SAML. מצאתי מספר מודולים, ומתוכם בחרתי את pysaml2. רציתי להשתמש תחילה במודול זה משום שהוא מאפשר לעבוד עם SAML, ליצור IDP, SP וכו'.

התחלתי ללמוד את השימוש במודול, אך לאחר מחשבה מעמיקה הבנתי שאעדיף לא להשתמש בו, אלא אוכל לבנות מערכת שצורת פעולתה דומה למבנה המוגדר בSAML, ללא שימוש במודול מיוחד לשם כך.

תיארתי מבנה מערכת חדש, שבו לא יהיה צורך במודול זה. שרטטתי גם תרשים זרימה שמתאר באופן רציף את תהליך פעולת המערכת. פירטתי בתרשים מה תבצע כל אחת מהתוכנות שהן חלק מהפרויקט שלי.

באמצעות התרשים התחלתי לכתוב את הקוד בצורה מסודרת. ראשית התחלתי מכתיבת הService Provider כולל ממשק המשתמש שלו. לאחר שזה מוכן והגרסא הראשונית שלו פועלת כראוי, התקדמתי לכתיבת הגרעין של המערכת – ה Identity Provider.

לאחר שבניתי מערכת הכוללת ממשק #C, הבנתי שעדיף יהיה לבנות את הפרויקט כך שהשרתים יהיו שרתי web. כלומר, הלקוח יהיה הדפדפן- באמצעות הדפדפן יפנה המשתמש אל שרת(SP) כלשהו, שיחזיר לו redirect לשרת ה IDP. שיטה זו נפוצה ויעילה יותר לדעתי מאשר אפליקציות בודדות עם ממשק #C, גם מפני שאפשר להפעיל שרת ולהתחבר אליו ממחשבים שונים באמצעות הדפדפן.

באמצעות תרשימים לתהליכים שארצה לממש בפרויקט שלי, הגדרתי סופית את המבנה והפרוטוקולים כאשר מדובר בשרתי web. במהלך בניית התרשימים נתקלתי במספר שאלות:

* *באחד מתהליכים אלו, אמור שרת הIDP להפנות את הלקוח בחזרה לשרת הSP. כיצד יפנה אותו בחזרה לשרת הנכון?*

ה SP צריך לשלוח לIDP מידע בנוגע לזהותו. דרך אחת לעשות זאת היא באמצעות שדה הhttp referrer. דרך נוספת היא באמצעות שליחת מזהה ייחודי של השרת המבקש, עם שליחת redirect. הדרך השלישית היא שליחת המזהה בנפרד, ישירות לשרת הIDP. אמנם בדרך זו המידע לא עובר דרך המשתמש ולכן התקשורת מאובטחת יותר, אך יש צורך בתקשורת נוספת עם השרת המרכזי, שעלולה להיות לא מתואמת מבחינת זמנים ונוחות. בחרתי להשתמש בדרך של שליחת מזהה מוצפן עם שליחת הredirect.

* *באיזה סוג הצפנה כדאי להשתמש?*

ראשית חשבתי להשתמש בהצפנה א-סימטרית, משום רמת האבטחה הגבוהה יותר. בהצפנה סימטרית יש צורך בהעברת מפתח, ולכן יורדת מידת האבטחה. אבל, במבט מעמיק יותר, שני הצדדים צריכים להצפין ולפענח מידע במערכת זו. לכן, יהיה יעיל יותר להשתמש בהצפנה סימטרית בכל זאת.

* *מתי ליצור וכיצד להעביר את מפתח ההצפנה בין שני השרתים?*

עבור כל שרת SP שמתחבר אליו, נחוך ל IDP מפתח קבוע. לכן, צריך להיות מנגנון של רישום SP, שבמהלכו יחליפו פרטים שני השרתים, וגם את מפתח ההצפנה. כך אין צורך בהחלפת מפתחות הצפנה בזמן שלקוח מתחבר, וגם לא בכל פעם מחדש.

* *כיצד לשמור את המידע על המשתמשים הרשומים?*

לצורך שמירת שמות המשתמשים והסיסמאות אשתמש ב SQLite3. כך גם לצורך התאמת מזהה המשתמש בין השרתים ולשמירת מידע של כל משתמש.

* *איך אבנה שרת web?*

התחלתי ללמוד את השימוש במודול flask לפייתון. מודול זה מאפשר בניית שרת web בשפת פייתון.

**בבליוגרפיה**

* MSDN, הרשת הרשמית של Microsoft למפתחים: <http://msdn.microsoft.com/library>
* הפורום הגדול ביותר לשאלות ותשובות בנושאי תכנות: [http://stackoverflow.com](http://stackoverflow.com/)
* התיעוד הרשמי של Python: [https://docs.python.org/2.7](https://docs.python.org/2.7/)
* אתר ללימוד Python: [http://www.tutorialspoint.com/python](http://www.tutorialspoint.com/python/)
* להורדת Python 2.7 (32-bit):

<https://www.python.org/ftp/python/2.7/python-2.7.msi>

* התקנת ספריית PyCrypto לפייתון Python 2.7 (32-bit): <http://www.voidspace.org.uk/downloads/pycrypto26/pycrypto-2.6.win32-py2.7.exe>
* התקנת מודול Flask לפייתון Python 2.7 (32-bit), באמצעות pip:

להתקין pip ולהריץ את הפקודה: pip install flask

* התקנת pip:

[https://pip.pypa.io/en/latest/installing](https://pip.pypa.io/en/latest/installing/)

* התקנת מודול sqlite3 לפייתון Python 2.7 (32-bit): <http://www.tutorialspoint.com/sqlite/sqlite_installation.htm>

**קוד הפרויקט**

מצוף כל הקוד של הפרויקט שלי:

**MyMainServerWeb**

*# region ---------------------- IMPORTS -------------------------***from** DataBaseManager **import** \*  
**from** Encryption **import** \*  
**from** ThreadWithReturnValue **import** \*  
**import** socket  
**from** flask **import** Flask, request, redirect, render\_template  
**import** thread  
**import** string  
**import** random  
*# endregion  
  
# region ------------------ CONFIGURATIONS ----------------------*DEBUG = True  
SECRET\_KEY = **'development key'**USERNAME = **'admin'**PASSWORD = **'default'**HOST = **'0.0.0.0'**PORT = 80  
DB\_NAME = **"MainDB.db"**MASTER = **b'Sixt33n Byt3 K3y'***# endregion*

*# region ---------------------- GLOBALS -------------------------*app = Flask(\_\_name\_\_)  
server\_sock = socket.socket()  
*# endregion*

*# region ------------------- URL\_FUNCTIONS ----------------------  
# route for handling the login page logic*@app.route(**'/login/<sp>'**, methods=[**'GET'**, **'POST'**])  
**def** login(sp):  
 error = None  
 **if** request.method == **'POST'**:  
 **try**:  
 *# find user in database* username = request.form[**'username'**]  
 password = request.form[**'password'**]  
 sp\_id = int(sp) *# add decryption* query = **"SELECT spUserID FROM Users WHERE username='%s' AND passw='%s' AND spID=%d"** %\  
 (username, password, sp\_id)  
 data\_base\_manager = DataBaseManager(DB\_NAME)  
 sp\_user\_id = data\_base\_manager.exec\_query(query)[0]  
 data\_base\_manager.close\_connection()  
 sp\_user\_id = get\_encrypt\_obj(sp\_id).encryptAES(str(sp\_user\_id))  
 sp\_url = **'%s/user/%s'** % (get\_sp\_url(sp\_id), str(sp\_user\_id))  
 **return** redirect(sp\_url)  
 **except** Exception, ex:  
 error = **'Invalid Credentials. Please try again.'  
 print** ex  
 **return** render\_template(**'LoginMain.html'**, error=error)  
  
  
*# route for handling the registration page logic*@app.route(**'/register/<userid> <sp>'**, methods=[**'GET'**, **'POST'**])  
**def** register(userid, sp):  
 **print** userid  
 **print "sp: "** + sp  
 sp\_id = int(sp)  
 sp\_userid = get\_encrypt\_obj(sp\_id).decryptAES(userid)  
 error = None  
 **if** request.method == **'POST'**:  
 *# add this user to database* username = request.form[**'username'**]  
 password = request.form[**'password'**]  
 confirm\_pass = request.form[**'confirmPassword'**]  
  
 **if** confirm\_pass == password:  
 data\_base\_manager = DataBaseManager(DB\_NAME)  
 user\_id = data\_base\_manager.last\_id(**"Users"**) + 1  
 data\_base\_manager.close\_connection()  
 add\_user(user\_id, username, password, sp\_id, sp\_userid)  
 sp\_userid = get\_encrypt\_obj(sp\_id).encryptAES(sp\_userid)  
 **return** redirect(get\_sp\_url()+**'/registeredas/'**+sp\_userid)  
 **else**:  
 error = **'Invalid Credentials. Please try again.'  
 return** render\_template(**'Register.html'**, error=error)  
*# endregion  
  
  
# region ------------------ OTHER\_FUNCTIONS ---------------------***def** get\_sp\_url(sp\_id=1):  
 query = **"SELECT redirectPath FROM SPs WHERE SPID=%d"** % sp\_id  
 **try**:  
 data\_base\_manager = DataBaseManager(DB\_NAME)  
 path = data\_base\_manager.exec\_query(query)[0]  
 data\_base\_manager.close\_connection()  
 **return** path  
 **except** Exception, e:  
 **print 'Unable to execute query: '** + query  
 **print** e  
  
  
**def** get\_encrypt\_obj(sid):  
 query = **"SELECT key FROM SPs WHERE SPID=%d"** % sid  
 data\_base\_manager = DataBaseManager(DB\_NAME)  
 key = data\_base\_manager.exec\_query(query)[0]  
 data\_base\_manager.close\_connection()  
 key = Encryption(MASTER).decryptAES(key)  
 **return** Encryption(key)  
  
  
**def** add\_user(id, username, passw, sp\_id, sp\_user\_id):  
 fields = [(id, username, passw, sp\_id, sp\_user\_id)]  
 data\_base\_manager = DataBaseManager(DB\_NAME)  
 data\_base\_manager.insert(**"Users"**, fields)  
 data\_base\_manager.print\_table(**"Users"**)  
 data\_base\_manager.close\_connection()  
  
  
**def** create\_db():  
 data\_base\_manager = DataBaseManager(DB\_NAME)  
 fields = [**"ID integer primary key autoincrement"**, **"username text not null"**, **"passw text not null"**,  
 **"spID integer not null"**, **"spUserID integer not null"**]  
 data\_base\_manager.create\_table(**"Users"**, fields)  
  
 fields = [**"SPID integer primary key autoincrement"**, **"details text not null"**, **"redirectPath text not null"**,  
 **"key text not null"**] *# , "encryptObj blob not null"]* data\_base\_manager.create\_table(**"SPs"**, fields)  
 data\_base\_manager.close\_connection()  
  
  
**def** generate\_random(size=16):  
 chars = string.ascii\_uppercase + string.ascii\_lowercase + string.digits  
 key = **''  
 for** i **in** range(size):  
 key += random.choice(chars)  
 **return** key  
  
  
**def** sps\_comm():  
 **while** True:  
 sp\_sock, sp\_addr = server\_sock.accept()  
 sp\_thread = ThreadWithReturnValue(target=register\_sp, args=(sp\_sock,))  
 sp\_thread.start()  
 fields = sp\_thread.join()  
 data\_base\_manager = DataBaseManager(**"MainDB.db"**)  
 data\_base\_manager.insert(**"SPs"**, fields)  
 data\_base\_manager.print\_table(**"SPs"**)  
 data\_base\_manager.close\_connection()  
  
  
**def** register\_sp(sp\_sock):  
 **try**:  
 sp\_sock.send(**'OK Send name redirectpath'**)  
 **print 'OK Send name redirectpath'** sp\_info = sp\_sock.recv(1024)  
 **print** sp\_info  
 sp\_name, sp\_server\_path = sp\_info.split(**'@'**)  
 new\_id = 1  
 key = generate\_random()  
  
 *# change encryption to Asymmetric* key2send = Encryption(**b'Sixteen Byte Key'**).encryptAES(key)  
 **print** key2send + **'@'** + str(new\_id)  
 sp\_sock.send(key2send + **'@'** + str(new\_id))  
  
 ans = sp\_sock.recv(1024)  
 **print** ans  
 **if not** ans.startswith(**'OK'**):  
 **raise** ValueError  
 sp\_sock.close()  
  
 key = Encryption(MASTER).encryptAES(key)  
 **return** [(new\_id, sp\_name, sp\_server\_path, key), ]  
   
 **except** Exception, e:  
 **print "ERROR"  
 print** e  
*# endregion  
  
  
# region ------------------------ MAIN --------------------------***def** main():  
 create\_db()  
  
 data\_base\_manager = DataBaseManager(DB\_NAME)  
 fields = [(1, **'elle'**, **'EL'**, 1, 101), (2, **'David'**, **'2511'**, 1, 102), (3, **'dana123'**, **'12345'**, 1, 103),  
 (4, **'dana123'**, **'12345'**, 2, 101), (5, **'elle'**, **'EL'**, 2, 102)]  
 data\_base\_manager.insert(**"Users"**, fields)  
 data\_base\_manager.print\_table(**"Users"**)  
 data\_base\_manager.print\_table(**"SPs"**)  
 data\_base\_manager.close\_connection()  
  
 server\_sock.bind((HOST, int(PORT)+1))  
 server\_sock.listen(5)  
 thread.start\_new\_thread(sps\_comm, ())  
   
 app.run(host=HOST, port=PORT)  
  
**if** \_\_name\_\_ == **'\_\_main\_\_'**:  
 main()  
*# endregion*

**MySPWEB:**

*# region ---------------------- IMPORTS -------------------------***from** DataBaseManager **import** \*  
**from** Encryption **import** \*  
**import** socket  
**from** flask **import** Flask, request, redirect, render\_template  
**import** netifaces  
*# endregion  
  
# region ------------------ CONFIGURATIONS ----------------------*DEBUG = True  
SECRET\_KEY = **'other development key'**USERNAME = **'admin'**PASSWORD = **'default pass'***#MAIN\_SERVER\_IP = '192.168.2.193'  
#MAIN\_SERVER\_IP = '10.0.0.9'*MAIN\_SERVER\_IP = **'84.109.203.199'**MAIN\_SERVER\_PORT = 80  
MAIN\_SERVER\_PATH = **'http://'** + MAIN\_SERVER\_IP + **':'** + str(MAIN\_SERVER\_PORT)  
HOST = **'0.0.0.0'**PORT = 8000  
*# endregion  
  
# region ---------------------- GLOBALS -------------------------*app = Flask(\_\_name\_\_)  
data\_base\_manager = DataBaseManager(**"PhoneBookDB.db"**)  
*# endregion  
  
  
# region ------------------- URL\_FUNCTIONS ----------------------*@app.route(**'/'**)  
**def** index():  
 **return** render\_template(**'PhoneBookIndex.html'**)  
  
  
*# route for handling the login page logic*@app.route(**'/login'**, methods=[**'GET'**, **'POST'**])  
**def** login():  
 error = None  
 **if** request.method == **'POST'**:  
 username = request.form[**'username'**]  
 password = request.form[**'password'**]  
 **if** username != **'admin' or** password != **'admin'**:  
 error = **'Invalid Credentials. Please try again.'  
 else**:  
 **return** redirect(**'/login/%s %s'** % (username, password))  
 **return** render\_template(**'LoginSP.html'**, error=error)  
  
  
@app.route(**'/login/<server>'**)  
**def** private\_login(server):  
 *# redirect to My Main Server* **if** server.lower() == **"mymainserver"**:  
 **return** redirect(MAIN\_SERVER\_PATH + **'/login/'** + str(my\_sp\_id))  
  
  
@app.route(**'/user/<userid>'**)  
**def** profile(userid):  
 *# show user profile* **try**:  
 userid = enc\_obj.decryptAES(userid)  
 **except** Exception, e:  
 **print** e  
 query = **"SELECT name, age, phoneNum FROM UserProfiles WHERE ID=%s"** % userid  
 name, age, phone\_num = data\_base\_manager.exec\_query(query)  
 **if** name:  
 **return** render\_template(**'Profile.html'**, name=name, age=age, phoneNum=phone\_num)  
 **else**:  
 *# error if userID was invalid* **pass**@app.route(**'/register'**)  
**def** register():  
 user\_id = data\_base\_manager.last\_id(**"UserProfiles"**) + 1  
 user\_id = str(user\_id)  
 user\_id = enc\_obj.encryptAES(user\_id)  
 **return** redirect(MAIN\_SERVER\_PATH+**"/register/"**+user\_id + **" "** + str(my\_sp\_id))  
  
  
@app.route(**'/registeredas/<user>'**, methods=[**'GET'**, **'POST'**])  
**def** registered(user):  
 user = enc\_obj.decryptAES(user)  
 error = None  
 **if** request.method == **'POST'**:  
 *# add this user to database* name = request.form[**'name'**]  
 age = request.form[**'age'**]  
 phone\_num = request.form[**'phoneNum'**]  
  
 **try**:  
 add\_user(user, name, age, phone\_num)  
 user = enc\_obj.encryptAES(user)  
 **return** redirect(**'/user/'**+user)  
 **except**:  
 error = **'Invalid Info. Please try again.'  
 return** render\_template(**'RegisterToSP.html'**, error=error)  
*# endregion  
  
  
# region ------------------ OTHER\_FUNCTIONS ---------------------***def** get\_my\_ip():  
 arr = []  
 interfaces = netifaces.interfaces()  
 **for** i **in** interfaces:  
 **if** i == **'lo'**:  
 **continue** iface = netifaces.ifaddresses(i).get(netifaces.AF\_INET)  
 **if** iface != None:  
 **for** j **in** iface:  
 *#print j['addr']* arr.append(j[**'addr'**])  
 **return** arr[4]  
  
  
**def** add\_user(id, name, age, phone\_num):  
 fields = [(id, name, age, phone\_num)]  
 data\_base\_manager.insert(**"UserProfiles"**, fields)  
 *#data\_base\_manager.print\_table("UserProfiles")***def** create\_db():  
 fields = [**"ID integer primary key autoincrement"**, **"name text not null"**, **"age integer not null"**,  
 **"phoneNum text not null"**]  
 data\_base\_manager.create\_table(**"UserProfiles"**, fields)  
 fields = [(101, **'Elizabeth'**, 17, **'09-8656735'**), (102, **'David'**, 10, **'03-1234567'**),  
 (103, **'Dana'**, 25, **'04-9182734'**)]  
 data\_base\_manager.insert(**"UserProfiles"**, fields)  
 *#data\_base\_manager.print\_table("UserProfiles")***def** save\_key\_id(key, my\_id):  
 key = Encryption(**b'Sixteen Byte Key'**).decryptAES(key)  
 enc = Encryption(key) *# correct enc\_obj: use to encrypt & decrypt sent data* my\_id = int(my\_id) *# send it for sp identification in redirect* **return** enc, my\_id  
  
  
**def** connect\_mymainserver():  
 my\_sock = socket.socket()  
 my\_sock.connect((MAIN\_SERVER\_IP, MAIN\_SERVER\_PORT+1))  
 ans = my\_sock.recv(1024)  
 **print** ans  
 **try**:  
 **if not** ans.startswith(**'OK'**):  
 **raise** ValueError  
 **print** ME  
 my\_sock.send(ME)  
 data = my\_sock.recv(1024)  
 key, my\_id = data.split(**'@'**)  
 my\_sock.send(**'OK End Connection'**)  
 my\_sock.close()  
 **return** save\_key\_id(key, my\_id)  
 **except** Exception:  
 my\_sock.send(**'Error'**)  
 my\_sock.close()  
*# endregion  
  
  
# region ------------------------ MAIN --------------------------*ME = **'PhoneBook'** + **'@'** + **'http://'** + get\_my\_ip() + **':'** + str(PORT)  
create\_db()  
enc\_obj, my\_sp\_id = connect\_mymainserver()  
  
  
**def** main():  
 app.run(host=HOST, port=PORT)  
 data\_base\_manager.close\_connection()  
  
**if** \_\_name\_\_ == **'\_\_main\_\_'**:  
 main()  
*# endregion*

**DataBaseManager:**

**import** sqlite3  
  
  
**class** DataBaseManager(object):  
  
 **def** \_\_init\_\_(self, name):  
 self.con = sqlite3.connect(name, )  
 self.cur = self.con.cursor()  
  
 **def** create\_table(self, table\_name, fields):  
 query = **"CREATE TABLE IF NOT EXISTS "** + table\_name + **"("  
 for** field **in** fields:  
 query += field + **','** query = query[:-1]  
 query += **")"** self.cur.execute(query)  
  
 **def** exec\_query(self, query):  
 self.cur.execute(query)  
 **return** self.cur.fetchone()  
  
 **def** insert(self, table\_name, fields):  
 query = **"INSERT INTO "** + table\_name + **" VALUES("  
 for** i **in** xrange(len(fields[0])):  
 query += **'?,'** query = query[:-1]  
 query += **")"** self.cur.executemany(query, fields)  
  
 **def** last\_id(self, table\_name):  
 rows = self.get\_rows(table\_name)  
 **return** int(rows[-1][0])  
 *# return self.cur.lastrowid* **def** get\_rows(self, table\_name):  
 self.cur.execute(**"SELECT \* FROM "** + table\_name)  
 rows = self.cur.fetchall()  
 **return** rows  
  
 **def** print\_table(self, table\_name):  
 rows = self.get\_rows(table\_name)  
 **for** row **in** rows:  
 **print** row  
  
 **def** get\_dict\_from\_table(self,table\_name):  
 *# Turn a list with sqlite3.Row objects into a dictionary* dictionary = {} *# the dictionary to be filled with the row data and to be returned* **for** i, row **in** enumerate(self.get\_rows(table\_name)): *# iterate throw the sqlite3.Row objects* fields = [] *# for each Row use a separate list* **for** col **in** range(0, len(row)): *# copy over the row date (ie. column data) to a list* fields.append(row[col])  
 dictionary[fields[1]] = (fields[2], fields[3]) *# add the list to the dictionary* **return** dictionary  
  
 **def** set\_dict\_to\_table(self,table\_name,dict):  
 keys = **','**.join(dict.keys())  
 i = 1  
 **for** word **in** dict.keys():  
 value = dict[word]  
 self.cur.execute(**"INSERT INTO "**+ table\_name +**" VALUES ("** + str(i) + **",'"** + word + **"',"** + str(value[0]) + **","** + str(value[1]) + **")"** )  
 i += 1  
 self.con.commit()  
  
 **def** close\_connection(self):  
 self.con.commit()  
 self.con.close()

**ThreadWithReturnValue:**

**from** threading **import** Thread  
  
  
**class** ThreadWithReturnValue(Thread):  
  
 **def** \_\_init\_\_(self, group=None, target=None, name=None, args=(), kwargs={}, Verbose=None):  
 Thread.\_\_init\_\_(self, group, target, name, args, kwargs, Verbose)  
 self.\_return = None  
  
 **def** run(self):  
 **if** self.\_Thread\_\_target **is not** None:  
 self.\_return = self.\_Thread\_\_target(\*self.\_Thread\_\_args, \*\*self.\_Thread\_\_kwargs)  
  
 **def** join(self):  
 Thread.join(self)  
 **return** self.\_return

**Encryption:**

**from** Crypto.Cipher **import** AES  
**import** base64  
  
  
**class** Encryption(object):  
  
 **def** \_\_init\_\_(self, key, enc\_type=**"AES"**, block=16):  
 self.\_\_cipher = AES.new(key)  
 self.encrypt\_type = enc\_type  
 self.block\_size = block  
 self.padding = **'{'  
  
 def** add\_padding(self, data):  
 num = self.block\_size - len(data) % self.block\_size  
 **return** data + num \* self.padding  
  
 **def** encryptAES(self, data):  
 padded = self.add\_padding(data)  
 encrypted = self.\_\_cipher.encrypt(padded)  
 encoded = base64.b64encode(encrypted)  
 final = self.remove\_slash(encoded)  
 **return** final  
  
 **def** decryptAES(self, encoded):  
 correct = self.add\_slash\_again(encoded)  
 decoded = base64.b64decode(correct)  
 decrypted = self.\_\_cipher.decrypt(decoded)  
 no\_padding = decrypted.rstrip(self.padding)  
 **return** no\_padding  
  
 **def** remove\_slash(self, data):  
 **while '/' in** data:  
 i = data.find(**'/'**)  
 data = data[:i] + **'$'** + data[i+1:]  
 **return** data  
  
 **def** add\_slash\_again(self, data):  
 **while '$' in** data:  
 i = data.find(**'$'**)  
 data = data[:i] + **'/'** + data[i+1:]  
 **return** data

**LoginMain:**

<html>

<head>

<title>Login page</title>

<meta name="viewport" content="width=device-width, initial-scale=1.0">

<link href="http://icons.iconarchive.com/icons/social-media-icons/glossy-social/512/Spring-me-icon.png" rel="shortcut icon">

</head>

<body>

<div class="container">

<center>

<h1>Please login</h1>

<br>

<form action="" method="post">

<input type="text" placeholder="Username" name="username" ><br/><br/><br/>

<input type="password" placeholder="Password" name="password" ><br/><br/><br/>

<input class="btn btn-default" type="submit" value="Login">

</form>

<!-- <form method="get" action="/register">

<input class="btn btn-default" type="submit" value="Register">

</form> -->

{% if error %}

<p class="error"><strong>Error:</strong> {{ error }}

{% endif %}

</center>

</div>

</body>

</html>

**Register: (Main)**

<html>

<head>

<title>Registration page</title>

<meta name="viewport" content="width=device-width, initial-scale=1.0">

<link href="http://icons.iconarchive.com/icons/social-media-icons/glossy-social/512/Spring-me-icon.png" rel="shortcut icon">

</head>

<body>

<div class="container">

<center>

<h1>Please enter credentials</h1>

<br>

<form action="" method="post">

<input type="text" placeholder="Username" name="username" ><br/><br/><br/>

<input type="password" placeholder="Password" name="password" ><br/><br/><br/>

<input type="password" placeholder="Confirm Password" name="confirmPassword" ><br/><br/><br/>

<input class="btn btn-default" type="submit" value="Register">

</form>

{% if error %}

<p class="error"><strong>Error:</strong> {{ error }}

{% endif %}

</center>

</div>

</body>

</html>

**PhoneBookIndex:**

<html>

<head>

<title>Welcome To PhoneBook</title>

<meta name="viewport" content="width=device-width, initial-scale=1.0">

<link href="http://www.isneo.org/wp-content/uploads/phonebook.png" rel="shortcut icon">

</head>

<body>

<center>

<h1>Hello Dear Guest!</h1>

<h2><strong>Welcome To PhoneBook!</strong></h2>

<p>We want to help you save your phone number.<br/>

During registration you will be asked to enter your name, age & phone number.<br/>

When logged in, we will show you these.</big></p>

<p><big>You don't have to worry about keeping your phone number in memory anymore!<br/>

Just log in and see it:</big></p>

<form method="get" action="/login">

<input class="btn btn-default" type="submit" value="Login">

</form>

<form method="get" action="/register">

<input class="btn btn-default" type="submit" value="Register">

</form>

<br/>

<img src="http://thumbs.dreamstime.com/t/phone-book-concept-public-35018949.jpg">

</center>

</body>

</html>

**LoginSP**

<html>

<head>

<title>Login page</title>

<meta name="viewport" content="width=device-width, initial-scale=1.0">

<link href="http://www.isneo.org/wp-content/uploads/phonebook.png" rel="shortcut icon">

</head>

<body>

<div class="container">

<center>

<h1>Please login</h1>

<br/>

<form action="" method="post">

<input type="text" placeholder="Username" name="username" ><br/><br/>

<input type="password" placeholder="Password" name="password" ><br/>

</form>

<form method="get" action="/login">

<input class="btn btn-default" type="submit" value="Login with username & password">

</form>

or<br/><br/>

<form method="get" action="/login/mymainserver">

<input class="btn btn-default" type="submit" value="Login with MyMainServer (preferable)">

</form>

{% if error %}

<p class="error"><strong>Error:</strong> {{ error }}

{% endif %}

</center>

</div>

</body>

</html>

**RegisterToSP:**

<html>

<head>

<title>Registration page</title>

<meta name="viewport" content="width=device-width, initial-scale=1.0">

<link href="http://www.isneo.org/wp-content/uploads/phonebook.png" rel="shortcut icon">

</head>

<body>

<div class="container">

<center>

<h1>Please enter your information</h1>

<br>

<form action="" method="post">

<input type="text" placeholder="Name" name="name" ><br/><br/><br/>

<input type="number" placeholder="Age" name="age" min="1" max="120"><br/><br/><br/>

<input type="text" placeholder="Phone Number" name="phoneNum" ><br/><br/><br/>

<input class="btn btn-default" type="submit" value="Register">

</form>

{% if error %}

<p class="error"><strong>Error:</strong> {{ error }}

{% endif %}

</center>

</div>

</body>

</html>

**Profile:**

<html>

<head>

<title>Your Profile</title>

<meta name="viewport" content="width=device-width, initial-scale=1.0">

<link href="http://www.isneo.org/wp-content/uploads/phonebook.png" rel="shortcut icon">

</head>

<body>

<center>

{% if name %}

<h1>Hello {{ name }}</h1>

<br/><br/><br/>

<p><big>Your name is: </big></p>

<big><strong> {{ name }} </strong></big><br/><br/><br/>

<p><big>Your age is:</big></p>

<big><strong> {{ age }} </strong></big><br/><br/><br/>

<p><big>Your phone number is: </big></p>

<big><strong> {{ phoneNum }} </strong></big><br/><br/><br/>

{% endif %}

</center>

</body>

</html>