**H&E**

**מגישות: הללי אלקלעי, עדן רובינץ**

**שנה: 2021**

**סמסטר: א'**

**מוסד: מרכז האקדמי לב**

**חוג: מדעי המחשב**

**מדריך: ברק עינב**

תוכן עניינים

[תיאור הפרויקט: 3](#_Toc66185414)

[**התהליך הכללי:** 4](#_Toc66185415)

[מטרת הפרויקט: 5](#_Toc66185416)

[עיצוב: 6](#_Toc66185417)

[**העברת המפתחות בזמן ההתקנה:** 6](#_Toc66185418)

[**זרימת התהליך הכללי ברשת:** 7](#_Toc66185419)

[**זרימת המידע בין ה TEE לHOST-** 7](#_Toc66185420)

[טבלת איומים: 8](#_Toc66185422)

[אופן עבודה: 9](#_Toc66185423)

[הרחבת הפרויקט: 9](#_Toc66185424)

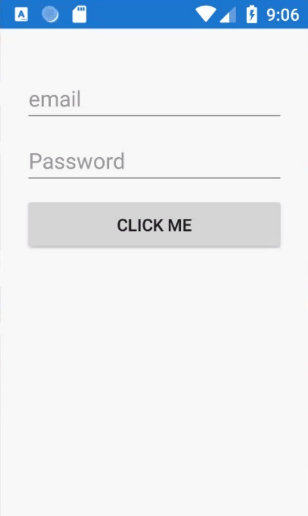
# תיאור הפרויקט:

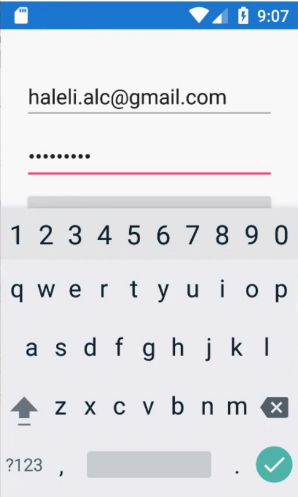
בפרוייקט זה רצינו לפתוח את המחשב בצורה חיצונית. (לא היה ניתן לבצע פתיחת מחשב לכן עשינו פתיחה של פייסבוק- יוסבר בהמשך)

לשם כך השתמשנו במפתחות א-סימטרים על מנת להצפין מפתח סימטרי וכך נוכל להעביר מידע ברשת בצורה בטוחה.

מבנה המערכת ע"פ המשתמש:

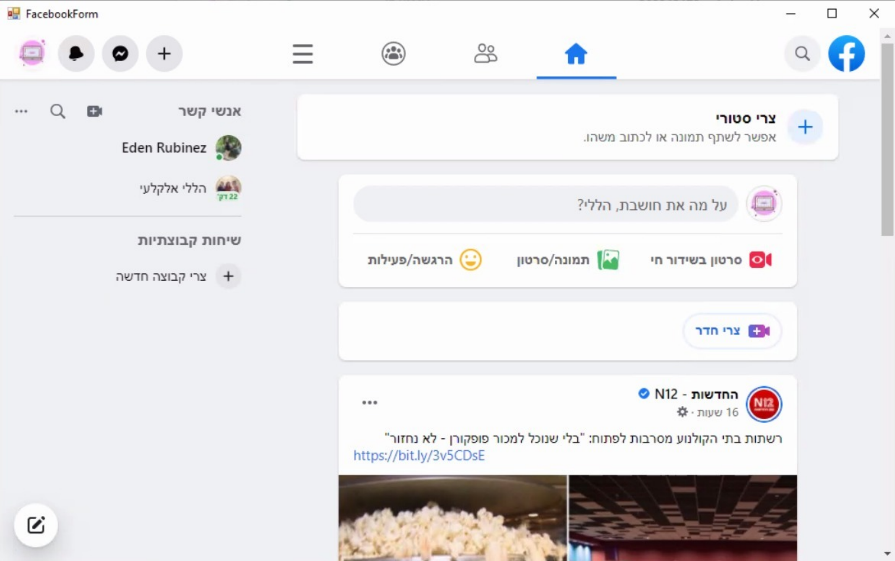
בשימוש הראשוני המשתמש צריך להוריד את האפליקציה ובנוסף להריץ את ה-HOST. לאחר ההרצה הראשונה יש לשנות את הconfig של ה-HOST על מנת שהוא יריץ מעכשיו את קטע הקוד של שאר התוכנית ( אם היינו מקמפלים את הקוד זה היה קורה אוטומטית אך מכיוון שהקוד לא מקומפל והוא רץ על Console application נצטרך לעשות זאת ידנית).

לאחר ההתקנה מתקבל המסך:

על המשתמש להכניס את שם המשתמש והסיסמא

של הפייסבוק שלו.

לאחר מכן ילחץ המשתמש על כפתור ה-CLICK שישלח את הנתונים שלו. אם ה-HOST על מצב ריצה הפייסבוק הרצוי יפתח על המחשב שלו.



## **התהליך הכללי:**

את המפתח הא-סימטרי יצרנו באפליקציה, יצרנו מפתח מסוג RSA בגודל 128 ביטים ל-mod ו3 ביטים ל-Ex, את המפתח הפרטי שמרנו באפליקציה ואת המפתח הציבורי העברנו לשרת והשרת שמר אותו במילון עם ID בתור KEY והמפתח הציבורי נשמר בתוך אובייקט (שמשמש כVALUE),בעל 2 שדות,אחד לציבורי ואחד למוצפן.

ה-HOST פנה לשרת עם ID זהה לזה של האפליקציה ושלף מהמילון את המפתח הציבורי. לאחר מכן ה-HOST פנה ל-APPLET (TEE) שיצור לו מפתח סימטרי השתמשנו במפתח מסוג AES אופן ההפעלה שהשתמשנו הוא ECB. ה-APPLET שמר את המפתח הסימטרי ב-FLASH וגם לקח העתק של המפתח הסימטרי והצפין אותו עם המפתח הציבורי.

את המפתח המוצפן ה-APPLET העביר ל-HOST שהעביר לשרת ששמר אותו באותו מילון עם אותו ID תחת שדה אחר.

האפליקציה פונה לשרת כדי לקחת את המפתח המוצפן ומפענחת אותו בעזרת המפתח הפרטי שלה ושומרת את המפתח הסימטרי.

עכשיו ל-APPLET ולאפליקציה יש דרך תקשורת מאובטחת.

ברגע שהמשתמש רוצה לפתוח את המחשב (במקרה שלנו את הפייסבוק) הוא מכניס את השם משתמש והסיסמא. בזמן הפתיחה השם משתמש, הסיסמא והזמן הנוכחי (השעה) עוברים הצפנה ונשלחים לשרת. במקביל ה-HOST המורץ פונה לשרת לקבלת המידע. המידע מועבר ל-TEE לפענוח, לאחר הפענוח הוא מעביר את המידע המפוענח ל-HOST והוא בודק אם הזמן שהועבר אליו היה בחמש דקות האחרונות. אם כן, הוא נותן אישור ופותח את המחשב (במקרה שלנו הפייסבוק)

# מטרת הפרויקט:

יצירת דרך נוחה לפתיחת מחשב בצורה חיצונית- את המחשב אפשר לפתוח באמצעות הסמארטפון וכך ניתנת גישה למחשב גם מרחוק.

המוצר שלנו בא לפתור בעיות אבטחה בכך שלא צריך להעביר את הסיסמא האישית לאנשים אחרים. בנוסף יש שליטה על המחשב האישי גם כשנמצאים במרחק.

לדוגמא: אמא שעובדת עד שעה מאוחרת. ילדיה שחוזרים מבית הספר נמצאים לבד בבית עד שהיא חוזרת. בזמן זה היא רוצה לתת להם גישה למחשב לזמן מוגבל מבלי לתת להם את הסיסמה.

באמצעות האפליקציה שכתבנו היא תוכל לפתוח את המחשב מרחוק וכך כולם יהיו מרוצים.

הפיתרון שיצרנו הוא יחודי , לא ראינו עוד פתרונות מסוג זה ובנוסף אנחנו מאמינות שהוא גם טוב ושימושי מכיוון שיצרנו מוצר מאובטח ואמין, את המפתח הסימטרי שמרנו הTEE וזה גורם לפרוייקט שלנו להיות יותר מאובטח מאשר פיתרונות אחרים שאולי דומים לפיתרון הזה.

# עיצוב:

## **העברת המפתחות בזמן ההתקנה:**

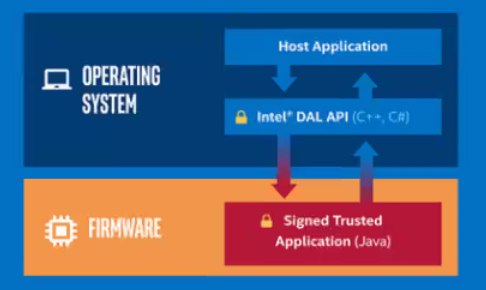
****

1. מהעברת מפתח ציבורי

4. העברת מפתח סימטרי מוצפן לפיענוח



2. העברת המפתח הציבורי למחשב

****

3. העברת מפצח סימטרי מוצפן

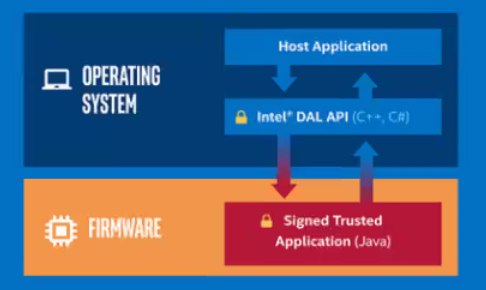
## **זרימת התהליך הכללי ברשת:**

****

מועבר שם משתמש , סיסמא, ושעה מוצפנים במפתח סימטרי

מועבר שם משתמש , סיסמא, ושעה מוצפנים במפתח סימטרי



****

## **זרימת המידע בין ה TEE לHOST-**

מועבר שם משתמש , סיסמא, ושעה מוצפנים במפתח סימטרי

HOST

TEE

מועבר שם משתמש , סיסמא, ושעה

# טבלת איומים:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Risk / Priority H, M, L | Attack Method and Attack Type or Surface | Asset (From asset table) | Adversary | Name | # |
| L | תקשורת בין DAL ולתצוגה  HOSTל-  וברשת וביישום הטלפון. | network server | Network Adversary  And  competitors | DOS | 1 |
| L | עובד ממורמר מתוך החברה יחבל במערכת ויגרום לבעיות מוצר.  העובד יחבל בפיתוח של המוצר. | DAL | Malicious Service Provider | Problem with an Intel product | 2 |
| M | התוקף יוצר Backdoor  ובעזרת זה יהיה ניתן לפרוץ למחשב ללא סיסמא. | Computer and phone | Skilled Hardware Adversary | Hardware attack | 3 |
| M | לקחת את הפלאפון ובעזרתו לפרוץ למחשב. | HOST and Computer | Unprivileged Software Adversary | Unauthorized entrance | 4 |

הפרוייקט שלנו מבוסס על TEE שלמדנו עליו במהלך הסמסטר, היתרון של שימוש בTEE לשמירת המפתח לאומת שמירה של המפתח על המחשב הוא ששמירה בTEE גורמת לכך שלא יהיה ניתן לפרוץ ולקחת את המפתח הסימטרי והשימוש בזה גורם לפרוייקט שלנו לשמור על סודיות ואמינות. בנוסף כל העברות ברשת הן בעזרת הצפנות וזה גורם לפרוייקט להיות יותר מאובטח.

# אופן עבודה:

את העבודה ביצענו יחד מפני שכך היה לנו יותר נוח.

אתגרים שהיו לנו במהלך הפרויקט:

כתיבת אפליקציה- דבר שלא עשינו לפני. היינו צריכות ללמוד מאפס איך לבנות אפליקציה קראנו מאמרים וראינו סרטונים המסבירים איך לעשות זאת.

כתיבת שרת- לא כתבנו שרת בסביבת .NET (פרט לתרגיל 5) וגם את זה היינו צריכות ללמוד מהתחלה.

פתיחת המחשב-חיפשנו הרבה באינטרנט איך לפתוח את המחשב וראינו הרבה אזהרות שלא לגעת ב-API של WINDOWS אלא אם כן יש לנו מערכת הפעלה לא בשימוש של WINDOWS. לכן קראנו המלצות על מעטפת ל-API שתפקידה לפתוח את המחשב בעזרת פונקציות של C#. הצלחנו לכתוב קוד שפותח את המחשב אך נוצרה לנו בעיה עם מעטפת זו מכיוון שהתוכנית שלנו רצה על EMULATE המעטפת שהשתמשנו בה לא יכולה להריץ את הקוד שנמצא ב-HOST. מכיוון שלא יכלנו לבצע את פתיחת המחשב עשינו במקום זה FORM שמעלה דף אינטרנט (במקרה שלנו פייסבוק) וניגש לשדות בדף ע"י שימוש בסקריפטים וכך פותח את הפרופיל האישי ששלחנו מהאפליקציה.

העבודה עם הTEE הייתה מאתגרת אך מעניינת, ובכללי כל העבודה עם הצפנות לפני הקורס הזה למדנו עליהם אופן תיאורתי בלבד אך בקורס הזה נכנס החלק המעשי, בהתחלה היה קשה להבין את כל התהליכים את כל העבודה עם ביטים, אחרי שהבנו זה נהיה מעניין יותר.

# הרחבת הפרויקט:

כמובן שיש עוד הרבה מה לשפר ולהוסיף:

1. אפשרות לסגור את המחשב ע"י האפליקציה
2. להגביל מראש את השימוש לזמן מסוים
3. שימוש ב-API של WINDOWS על מנת לפתוח את המחשב.
4. אפשרות להכניס טביעת אצבע במקום הקלדת שם משתמש וסיסמא