**Teurse מסמך עיצוב**

נכתב ע"י: גבי אברמוביץ

אלינה לוי

יעקב טורצקי

תאריך: 17.11.2013

גרסה: 1.2

|  |  |  |  |
| --- | --- | --- | --- |
| שונה ע"י | מהות השינוי | תאריך | גרסה |
| כולם | תיקונים | 17.11.13 | 1.00 |

**תיאור כללי**

הפרויקט  הינו סוס טרויאני המושתל על מכשירים בעלי מערכת הפעלה Android, גרסאות 2.2 עד 4.3.1.

המודל הכללי הינו מודל שרת-לקוח. השרת הינו אתר אשר יש להתחבר אליו עם שם משתמש וסיסמא. דרך האתר ניתן לראות מידע שנאסף בצד הלקוח וגם לאפשר שליחה של פקודות מהמשתמש, לדוגמא שליחת אסמס, ביצוע שיחה, הוספת קובץ ועוד.

**מבני נתונים**

* טבלת אנשי קשר: מכילה את הרשומות הרלוונטיות (TBD) לכל איש קשר.
* טבלת יומן שיחות: רשימת השיחות וההקלטות שלהם.
* טבלה נתונים אודות הפלאפון – מספר גרסה , מספר פלאפון ועוד.
* טבלת SMS: מכילה מידע על כל SMS שנשלח או התקבל.
* טבלת הגדרות המכשיר: מכילה רשימה של כל ההגדרות הקיימות במכשיר.
* טבלת אירועים מלוח שנה: מכילה את כל האירועים הנמצאים בלוח השנה של המכשיר.
* קובץ ובו רשימה של קבצים ותיקיות.
* טבלת אפליקציות מותקנות.
* טבלה אשר מצביעה לרשימת קבצים + הקבצים עצמם (יכווצו בעת משלוח).
* טבלת מיקומי GPS.

מבני הנתונים הנ"ל רלוונטיים גם לצד לקוח וגם לצד שרת

**לוגיקת תוכנית**

לקוח

* שליחת מידע: הלקוח ניגש אל כתובת הWEB של השרת (לדוגמא: evil-site.com/gateway.php?send) ושולח את המידע הרצוי.
* קבלת מידע: הלקוח ניגש אל כתובת הWEB של השרת (לדוגמא: evil-site.com/gateway.php?receive) ומקבל את המידע הרצוי עפ"י הID שלו.
* לאחר התקנה: בדיקת Anti-Emulation –נבדוק האם התוכנה מופעלת על מדמה -אם כן, השבתה של התוכנה, אם לא - נמשיך הלאה.
* לאחר התקנה: במידה ויש גישה לאינטרנט - שליחת התרעה לאתר. בתוך ההתרעה יהיה מידע התחלתי אודות הטלפון, מצב סוללה, מיקום GPS וכדומה.
* כל פעם שיש חיבור לאינטרנט - מידע חדש נשלח לשרת, והטבלאות מתעדכנות.
* כיווץ כל המידע בטרם שליחתו (המרת תמונות לרזולוציה נמוכה\הקלטות MP3 באיכות נמוכה)
* במידה והחיבור הופסק בעת העברת המידע - שליחה מחדש לאחר חידוש החיבור.
* קריאת גיבויים מן הזיכרון של המכשיר.
* Privilege Escalation: ע"י השגת ROOT או Device Administration.

|  |  |
| --- | --- |
| **פרטי הפונקציה:** | **שם פונקציה:** |
| מבצע: שולח מידע לשרת | Boolean SendDataToServer(string data) |
| מחזיר: אמת במקרה הצלחה ושקר במקרה כישלון |
| מבצע: מקבל מידע מהשרת | Boolean ReiciveDataFromServer() |
| מחזיר: אמת במקרה הצלחה ושקר במקרה כישלון |
| מבצע: שולח קובץ לשרת בצירוף מידע על הקובץ | Boolean SendFile(string location, string name, string info) |
| מחזיר: אמת במקרה הצלחה ושקר במקרה כישלון |
| מבצע: יוצר רשומה עם מידע חדש במסד הנתונים | Boolean SaveToDatabase(string dbname, string tablename, string data) |
| מחזיר: אמת במקרה הצלחה ושקר במקרה כישלון |
| מבצע: | Tbd GetFromDatabase( string dbname, tablename, id) |
| מחזיר: את הרשומה המבוקשת |
| מבצע: מעדכן רשומה | UpdateRecordeInDatabase (dbname, tablename, id, data) |
| מחזיר: אמת במקרה הצלחה ושקר במקרה כישלון |
| מבצע: מוחק רשומה מהמסד | DeleteFromDatabase(dbname, tablename, id) |
| מחזיר: אמת במקרה הצלחה ושקר במקרה כישלון |
| מבצע: בודק את מצב הפלאג בלופ | ListenToFlag(FlagName) |
| מחזיר: אמת במקרה והפלאג נדלק ושקר במקרה שהוא מכובה |
| מבצע: פונקציה רקורסיבית שעוברת על רשימת התיקיות והקבצים בתיקייה | GetFilesTree(dir) |
| מחזיר: רשימת תיקיות, תתי-תיקיות וקבצים במערך |
| מבצע: קורא קובץ | ReadFromFIle(location, name) |
| מחזיר: את ה-data שנמצא בקובץ |
| מבצע: יוצר קובץ חדש | AddFile(location, name) |
| מחזיר: אמת במקרה של הצלחה, שקר במקרה של כישלון |
| מבצע: כותב מידע לקובץ קיים (אם הקובץ לא קיים נקרא לפונקצייה Addfile | WriteToFile(location, name, data) |
| מחזיר: אמת במקרה של הצלחה,שקר במקרה של כישלון |
| מבצע: מוסיף תקייה | AddDir(location, name) |
| מחזיר: אמת במקרה הצלחה ושקר במקרה כישלון |
| מבצע: מוחק את תקייה | RemoveDir(location, name) |
| מחזיר: אמת במקרה הצלחה ושקר במקרה כישלון |
| מבצע: שולח sms | SendSMS(phoneNumber,data) |
| מחזיר: אמת במקרה הצלחה ושקר במקרה כישלון |
| מבצע: מקליט שיחה | RecordCall() |
| מחזיר: אמת במקרה של הצלחה,שקר במקרה של כישלון |
| מבצע: | GetGpsInfo() |
| מחזיר: את פרטי המיקום של הלקוח |
| מבצע: | GetNetworkStat() |
| מחזיר: את סוג הרשת שהמשתמש מחובר אליה |

שרת

* המשתמש מתחבר לאתר.
* האתר מציג לו מידע.
* הצגת מידע עפ"י החשיבות שלו (פרמטרים מוגדרים מראש, תדירות השימוש וכו').
* מחיקת מידע מהלקוח.
* שליחת מידע אל הלקוח (קבצים\תוכנות\פקודות לביצוע).
* מחיקת מידע מהשרת.
* בקשת קובץ מן הלקוח.

|  |  |
| --- | --- |
| תכונות | שם עצם |
| String FirstName | contact |
| String LastName |
| String PhoneNumbe –(list) |
| String Mail |
| String Organization |
| String Data | Sms |
| String PhoneNumber |
| Time time |
| Gps location |
| String PhoneNumber | Call |
| Integer Type |
| Time Time |
| String CallDuration |
| Gps location |
| String Name | Call Record |
| Gps Location |
| Time Time |
| Time CallDuration |
| String Name | ApplicationData |
| String Version |
| String installationDate |
| String PackageName |
| String LastUseDate |
| Integer Size |
| Integer Day | Time |
| Integer Month |
| Integer Year |
| Integer Hour |
| Integer Minute |
| Integer Second |
| String Name | Event |
| time Starttime |
| Time duration |
| String Place |
| String Description |
| Contact contactlist |
| String data | NFC |
| Gps location |
| Integer Longitude | GPS |
| Integer Latitude |
| Integer height |
| Integer speed |

אופן החיבור בין צד הלקוח לצד השרת

***חיבור בפעם הראשונה:***

לקוח

לקוח

שרת

שליחת פרטים בסיסים

הודעת אישור על קבלת המידע ושליחת סיסמא

הלקוח עובר לנוהל הרגיל

שליחת פרטים בסיסים- פרטים טכניים על המכשיר (מעבד , דגם ,RAM , גירסת מכשיר ומידע טכני על הסים).

הודעת אישור על קבלת המידע ושליחת סיסמא – השרת מודיע ללקוח שהוא קיבל את המידע והוא שולח לו סיסמא (כדי להתחבר עליו לשלוח גם את הסיסמא שלו וגם מידע בסיסי על המכשיר).

***נוהל רגיל:***

שליחת ה-ID והסיסמא

שרת

לקוח

לקוח

ZZZ

הודעת אישור

קבלת רשימת מטלות

שליחת מידע

שליחת ה-ID והסיסמא : הלקוח שולח לשרת את ה-HASH שהוא מחזרות עם כל המידע הבסיסי של המכשיר ובנוסף שולח לו סיסמא שאותה קיבל בחיבור הראשון.

הודעת אישור : השרת מאשר כי כל הפרטים נכונים ושיש חיבור בין השרת ללקוח.

קבלת רשימת מטלות :אם יש מטלות לביצוע הוא מבצע אותן.

שליחת מידע: הלקוח שולח מידע אל דף מסוים בשרת (כל מידע חדש שישנו בפלאפון הלקוח שולח לשרת).