בס״ד

האוניברסיטה הפתוחה

המחלקה למתמטיקה ולמדעי המחשב

החטיבה למדעי המחשב

אפיון פרויקט גמר

פרוטוקולים מאובטחים למימוש ארנק דיגיטלי מבוסס קול

מנחה: פרופ׳ אהוד גודס

מגיש:

לירן רופמן

ת״ז- 021954672

תקציר

פתרון הארנק הדיגיטלי אשר ממומש ע״י תמסורת קול הינו פתרון אשר מתפתח אט אט ותופס מקום מרכזי יותר במשפחת הפתרונות לארנק הדיגיטלי. זאת במיוחד מפאת העובדה שמדובר בטכנולוגיה זמינה לכל שמצריכה סה״כ מיקרופון ורמקול המותקנים בכל טלפון. פתרונות פופולאריים יותר לארנק דיגיטלי, כדוגמת פתרון ה-NFC (Near Field Communication/תקשורת טווח אפס) [1], דורשים הימצאות של רכיב ייעודי בטלפון אשר מתבסס על RF (Radio Frequency).

אך העניין האקדמי בניתוח העברת מידע באמצעות צליל, והסיבה שבחרנו בלהתמקד בתווך זה באופן ייחודי, נובע מטבעו הלא מאובטח של התווך מחד, ומחוסר האמינות שלו מאידך הנובעים מהאופי הפיסיקלי של תמסורת הקול. ניכר כי השילוב של שתי תכונות אלו נותן עניין רב למחקר סביבו.

למרבה ההפתעה, רובם המכריע של המימושים לארנק דיגיטלי הקיימים בשוק, המבוססים על שימוש בתמסורת קול, מצריכים גישה חיצונית לאינטרנט של מכשיר הקונה לצורך ביצוע העסקה. זוהי חריגה חדה מפתרונות הארנק הדיגיטלי הקלאסי כגון NFC, אשר אינם מסתמכים על חיבור שכזה. בנוסף, זוהי דרישת סף שבמקרים מסוימים לא מתאפשרת ע״י הקונה.

פרויקט גמר זה מהווה את חלק המימוש של העבודה המסכמת: ״פרוטוקולים מאובטחים למימוש ארנק דיגיטלי מבוסס קול״.

הדגש המרכזי בעבודה המסכמת ניתן לסקירה וניתוח של סוגי ארנקים דיגיטליים מבוססי תמסורת קול אשר אינם מסתמכים על קיומה של קישוריות המאפשרת גישה חיצונית לשרתי ספק שירות התשלומים. הסיבה לכך היא שארנק דיגיטלי מסוג זה מחייב העברה רבה יותר של נתונים בעלי רגישות אבטחתית גבוהה, על גבי תמסורת הקול, ובשל כך סוג זה מהווה אתגר מעניין למציאת פתרונות להעברת הנתונים באופן מאובטח.

פרויקט זה מביא למימוש שני פרוטוקולים מייצגים מאלו אשר תוארו בעבודה המסכמת (פתרון ההצפנה האסימטרית בתוספת שימוש בתעודה דיגיטלית ופתרון Time-based One-time Password משולב עם גיבוב מידע). כל פרוטוקול מייצג אסכולת אבטחה משל עצמו. אם בעבודה המסכמת התמקדנו בניתוח האבטחתי ובמתקפות פוטנציאליות על הפרוטוקולים, בפרויקט זה אנו מדגימים את היתכנותם בפועל, משווים בין ביצועיהם ומנתחים היבטי חווית משתמש אשר קשורים ליכולתנו הלכה למעשה, להשתמש בהם ליישומים מעשיים.

1. רקע

נגדיר את המונח 'עסקה אלקטרונית' בתור כל עסקה אשר מתבצעת בין קונה ומוכר על גבי תקשורת אלקטרונית באמצעות גורם מתווך (שרת סליקה). הגדרה זו עומדת בניגוד גמור לעסקה מסורתית אשר מתקיימת באמצעות תשלום כסף מזומן ללא צורך בגורם מתווך. אם כך, מתבהר כי במשך עשורים שלמים כרטיס האשראי היה האמצעי הבלעדי והמוחלט לביצוע עסקאות אלקטרוניות.

בהיבט חוויית השימוש, כרטיס האשראי מחייב הרי נשיאה של חפץ (ארנק), ובמשך שנים נראה היה כי אין טעם בלמצוא לו תחליף שיהווה בשורה התחתונה החלפת חפץ אחד באחר.

בשנים האחרונות, במקביל להתפתחויות שהתבצעו בעולם התקשורת הסלולארית, בהם כניסתם של הטלפונים החכמים לשוק, החל להתפתח תחום חדש בעולם העסקאות האלקטרוניות בשם 'ארנק דיגיטלי'.

כיום כמעט כל אדם נושא על גופו סוג של מחשב זעיר אשר ביכולתו להתחבר באופן מאובטח לשרתים מרוחקים. גורמים פרטיים רבים, ובהם בעיקר יצרני טלפונים חכמים וחברות האשראי המסורתיות, הבינו במהרה את הפוטנציאל העסקי הגלום בכך, והחלו לפתח פתרונות שונים ויצירתיים המאפשרים שימוש בטלפון החכם האישי כארנק דיגיטלי.

אחד העקרונות המנחים במימוש פתרון לארנק דיגיטלי הוא כי לכל הפחות לא תהיה ירידה בחוויית הקניה של הקונה וברמת האבטחה לעומת שימוש בתשלום באמצעות כרטיס אשראי. פתרון ארנק דיגיטלי טוב יציג אף שיפור בשני רבדים אלו.

כאשר ננתח את הבסיס המשותף לפרוטוקולים המשמשים לצורך ביצוע עסקה אלקטרונית (נכללים בהגדרה זו גם כרטיס האשראי וגם הארנק הדיגיטלי), ניתן להיווכח כי תמיד ישנם בנמצא 4 גורמים מעורבים-

i. **קונה**- האדם אשר יוזם את העסקה ומעוניין להעביר למוכר כסף תמורת מוצר מסוים. בעסקאות שאינן מבוססות על מזומן, ע"מ לקיים את העסקה, הקונה לרוב משתמש באמצעי אשר מעביר למוכר מידע נדרש על חשבונו של הקונה ע"מ לבצע את התשלום (כרטיס אשראי לדוגמא).
ii. **מוכר**- האדם בבית העסק אשר מקיים את האינטראקציה עם הקונה. המוכר יכול להיות בעל העסק בעצמו או לחילופין נציג בעל העסק, לדוגמא- קופאי.
iii. **מכשיר המוכר**- המכשיר בו המוכר משתמש ע"מ לאמת את זהותו של הקונה ולבצע לבסוף את העסקה. מכשיר המוכר מתקשר באופן שוטף עם שרת הקצה של ספק שירות התשלום, באמצעות תקשורת זו מוודא אל מול שרת הקצה את זהותו של הקונה ואת יכולתו לשלם (מסגרת אשראי) ומורה לשרת הקצה לבצע לבסוף את העסקה בפועל. לדוגמא, בעת תשלום באמצעות כרטיס אשראי, מכשיר המוכר 'יגהץ' את הכרטיס ויעביר את נתוני הקונה לעבר שרת הקצה של ספק שירות התשלום (במקרה הזה, יהיה מדובר בשרת חברת האשראי או חברת הסליקה). השרת יוודא כי הקונה קיים במאגר ושיש לו מסגרת אשראי מתאימה ורק אז יבצע את פעולת התשלום בפועל.

צורה נוספת לראות את תפקידו הוא שמכשיר המוכר הוא למעשה מתווך בין אמצעי התשלום של הקונה לבין שרת הקצה של ספק שירות התשלומים.

iv. **שרת הקצה**- נשתמש בהגדרה 'שרת קצה' ע"מ להגדיר כשם כללי את כלל השרתים אותם מתחזק ספק שירות התשלום (חברת האשראי או החברה נותנת שירות הארנק הדיגיטלי). בין שרתי הקצה של ספק השירות ניתן למצוא את השרת שמכשיר המוכר מתקשר מולו, שרת מסד הנתונים אשר מחזיק את נתוני כלל הלקוחות והעסקים הרשומים לשירות, שרת הסליקה שמבצע את העסקה בפועל וכו'.

פתרון הארנק הדיגיטלי, כפי ששמו מרמז, דוחף אותנו להכניס גורם חדש (וחמישי) לפרוטוקול העסקה. אותו גורם מחליף את כרטיס האשראי המסורתי במכשיר אלקטרוני אישי בו הקונה משתמש כאמצעי עזר ע"מ לבצע את העסקה. נכנה את גורם זה בשם הכללי- 'מכשיר הקונה'.

למרות שבעבר היו מספר מימושים שונים למכשיר זה, כיום ברוב המוחלט של הפתרונות, כאשר מדברים על מכשיר הקונה, מתייחסים לרוב למכשיר טלפון חכם. האמצעי בו הטלפון החכם מסוגל לבצע את הפעולות הנדרשות ממנו כחלק מפרוטוקול העסקה מתבצע באמצעות אפליקציה ייעודית המותקנת על המכשיר אשר ניתנה לקונה ע"י ספק שירות התשלומים. באמצעות מסך המכשיר אשר משמש גם כמסך מגע, הקונה מסוגל לשלוט בפעולתה של אותה אפליקציה בזמן העסקה (לדוגמא- לבחור מספר תשלומים רצוי) ולקבל חיוויים רלוונטיים (מחיר העסקה, האם העסקה אושרה או נכשלה וכו').

בעבודה המסכמת התוודענו ליתרונותיו של הארנק הדיגיטלי. כאשר משווים אותו ראש בראש עם כרטיס האשראי, ניכר כי הארנק הדיגיטלי, לכל הפחות, שומר על כלל יתרונות כרטיס האשראי ואף מהווה שיפור הן מבחינה אבטחתית והן מבחינת חוויית המשתמש. אך בכל זאת, לא ניתן להתעלם משלושה חסרונות בולטים הקיימים במימושי ארנק דיגיטלי מבוססי תמסורת RF-

- כפי שהדגמנו בעבודה המסכמת, פתרון NFC (שאליו נתייחס לצורך העניין כמייצג של פתרונות מבוססי תמסורת RF) אינו מוגן באופן מספק ממתקפת 'אדם באמצע'.
- נכון להיום, חומרת ה-NFC אינה נפוצה דיה. מבין המכשירים החכמים אשר נמכרו ב-2013 רק 18.2% מכילים את חומרת ה-NFC. לפי התחזיות, עד 2018 המספר אמור לעלות עד ל-64% [23]. אך צריך כי נתונים אלו מדברים רק על מכירה של טלפונים חדשים, ולכן סביר להניח כי הנתונים לגבי התמיכה ב-NFC עבור כלל הטלפונים אשר בידי הציבור הרחב נמוכים הרבה יותר.
- תמסורת RF ניתנת להעברה אך ורק באופן ישיר ובלתי אמצעי- התמסורת איננה ניתנת להעברה דרך הטלפון, ולכן לא ניתן לבצע באמצעות הטכנולוגיה רכישה דרך הטלפון (או באמצעות תוכנות חלופיות לטלפון כגון Skype).

לעומת זאת, ניכר שארנק דיגיטלי המבוסס על תמסורת קול יכול להתגבר על מגבלות אלה. יתרונות השימוש בתמסורת קול על פני שימוש בתמסורת RF-

- לא מצריכה חומרה מיוחדת. בכל טלפון סלולארי לצורך העניין קיימים מיקרופון ורמקול [24].

- בנוסף לשימוש הקלאסי בארנק דיגיטלי מבוסס תמסורת הקול באופן בלתי אמצעי, תמסורת הקול ניתנת להעברה גם דרך טלפוניה (או באמצעות תוכנות חלופיות לטלפון כגון Skype), ובכך מאפשרת ביצוע רכישות מרוחקות ללא תלות במרחק הפיסי של הקונה ממיקום בית העסק ע״י העברת תמסורת הקול דרך השיחה עצמה [25].
- ניכר כי היתרון המרכזי של פתרון הארנק הדיגיטלי מבוסס תמסורת קול הוא שבתצורות מסוימות של הפתרון, כפי שנראה בהמשך, הוא עמיד בצורה יפה למתקפת ׳אדם באמצע׳, בניגוד לפתרון מבוסס NFC.

2. מטרת הפרויקט ודרישות המערכת

מטרת המערכת אשר נבנתה בפרויקט זה היא הבאה למימוש שניים מהפתרונות לארנק דיגיטלי מבוסס קול, אשר יתוארו בפירוט בהמשך המסמך-

- פתרון ההצפנה האסימטרית בתוספת שימוש בתעודה דיגיטלית
- פתרון Time-based One-time Password משולב עם גיבוב מידע

פרוטוקולים אלה הם רק שניים מבין פרוטוקולים רבים אשר תוארו בעבודה, אך הם מהווים פתרון מייצג עבור כל אחת משתי אסכולות הפתרון אשר תוארו- פתרונות מבוססי הצפנה ופתרונות מבוססי token תלוי זמן.

המערכת תבנה בדמות יישומון (אפליקציה) למע״ה ׳אנדרואיד׳ אשר יעוצב כך שמתוך היישומון ניתן יהיה להפעיל ולדמות את-

- מכשיר הקונה
- מכשיר המוכר
- שרת הקצה

השיטה בה נרצה להדגים את פעולת הפרויקט תהיה ע״י שימוש במספר מכשירים פיסיים שונים במקביל, אשר יעבירו ביניהם מסרים על גבי תווך צליל. ההנחה היא כי החלק המדמה את מכשיר המוכר והחלק המדמה את מכשיר הקונה יופעלו על שני מכשירים פיסיים שונים. למרות שבעולם האמיתי, שרת הקצה יורץ תמיד כישות נפרדת ומרוחקת, בכדי להקל את תהליך ההדגמה, אכן נאפשר הרצה של תהליכון שרת הקצה על מכשיר נפרד, אך נאפשר הרצה גם על גבי אחד מהמכשירים האחרים (מכשיר הקונה או מכשיר המוכר).

דרישות מערכת נוספות-

- מסד נתונים- בשרת הקצה נשתמש גם במסד נתונים אשר יאגור את נתוני הלקוחות השונים (מוכרים וקונים).
- חיבור תקשורת-

- שרת הקצה- בהאזנה מתמדת לתשדורת HTTP נכנסת.
- מכשיר המוכר- פותח session יוצא של HTTP לעבר שרת הקצה בזמן ביצוע עסקה פעילה.
- מכשור הקונה- פותח session יוצא של HTTP לעבר שרת הקצה אך ורק בזמן תהליך ההרשמה לשירות. ז״א פעם אחת ולא בכל קניה, מה שמייתר את הצורך בחיבור תקשורתי מצד מכשיר הקונה בזמן ביצוע עסקה.

3. אבני יסוד

3.1. סימוני מסרים בסיסיים

נגדיר מספר סימונים לסוגי מסרים בסיסיים אשר כפי שציינו אמורים לעבור באמצעות תמסורת צלילים (ישנם גם סוגי מסרים נוספים שאותם נגדיר בהמשך).

כמו כן, נגדיר את מספר הסיביות של כל מסר למעט אלו שאינם עוברים באמצעות תמסורת הקול-

סימון	מספר תווים	תיאור
TransPrice	**8**	**מחיר העסקה (כולל סוג המטבע בו מתבצעת העסקה)**
BusinName	12	שם בית העסק
MaxPmt	**2**	**מספר התשלומים המקסימלי האפשרי**
ChosenPmt	2	מס׳ התשלומים שנבחרו ע״י הקונה
BuyerConfirmation	**1**	**אישור/דחיית העסקה מצד הקונה**
ServerConfirmation	-	אישור/דחיית העסקה מצד שרת הקצה
BuyerId	**8**	**המזהה החח״ע (חד-חד ערכי) של הקונה**
SellerUser	-	זהות המשתמש באמצעותו מכשיר המוכר מתחבר לשרת הקצה
SellerPassword	**-**	**הסיסמא באמצעותה מכשיר המוכר מתחבר לשרת הקצה**

3.2. סימוני פונקציות יסודיות

נגדיר מספר פונקציות אשר יסייעו לנו בהמשך-

- **S_n(M1,M2,…)** – המסרים M1,M2,… ישלחו באמצעות תמסורת צלילים. בתחילת השדר ובסופו יתווספו צלילים יעודים המשמשים כעזר שידור. כמו כן, יוצמד מזהה שדר בעל ערכים אפשריים של

1-3 כעזר הנועד לזהות את סוג השדר. בנוסף, יתווסף צליל אשר ישמש כסיכום ביקורת. כל אחד משלושת סוגי השדרים מייצגים את שלושת שלבי שליחת תמסורות הקול (יפורט בהמשך).

- **N_{URI}(M1,M2,…)** – המסרים M1,M2,… ישלחו דרך תמסורת הרשת. נסמן כ-URI את הכתובת אליה מתבצעת הפניה.
- **V(M)** – המסר M ישלח לעבר צג המוכר.
- **P(M)** – המסר M ישלח לעבר צג הקונה.

3.3. מילון מונחים

נגדיר בקצרה מספר מושגי יסוד הנוגעים לפיתוח יישומונים במע"ה Android-

א. **יישומון (אפליקציה)**- התוצר הסופי של הפרויקט. בפרויקט זה היישומון ייכתב בשפת Java for Android ע"מ שיוכל לרוץ במע"ה Android.

ב. **Activity**- כך מכונה כל מסך ביישומון Android.

ג. **Fragment**- לצורך הפשטת הקוד ניתן לחלק כל Activity לחלקים קטנים יותר ולפתח מסכים על גביהם. Fragment מוצג בסופו של דבר באזור מוגדר בתוך ה-Activity.

4. פתרונות לארנק דיגיטלי מבוסס תמסורת קול

כעת נתאר את אופן הפעולה של שניים מהפתרונות לארנק דיגיטלי מבוסס קול אשר תוארו בפירוט בעבודה המסכמת. מבין שלל הפתרונות אשר תוארו בעבודה, נבחרו שני אלה מתוך היותו של כל אחד מהם המאובטח ביותר בתוך אסכולות הפתרון-

- פתרון מאסכולת ההצפנה- פתרון ההצפנה האסימטרית בתוספת שימוש בתעודה דיגיטלית
- פתרון מאסכולת השימוש ב-Token- פתרון Time-based One-time Password (TOTP) משולב עם גיבוב מידע

4.1. פתרון ההצפנה האסימטרית בתוספת שימוש בתעודה דיגיטלית

המשותף לשני הפתרונות הקודמים הוא שהאתגר המרכזי שהם ניסו להיענות לו הוא הסתרת הנתון הסודי של מספר כרטיס האשראי של הקונה בעת העברתו ממכשיר הקונה למכשיר המוכר. התחוור לנו כי גם הפתרון בו הנתון הסודי עובר באופן מוצפן איננו חסין מפני מתקפת 'אדם באמצע'.

יתכן כי עצם ההגדרה של האתגר שעומד לפנינו היא זו שהיתה שגויה מלכתחילה? מסתמן כי די בשליחתו של נתון סודי בין שני רכיבים אשר לא קיימת ביניהם כל היכרות מוקדמת בכדי להפוך את הפתרון לחדיר למתקפה מסוג 'אדם באמצע'. ננסה מעתה לשנות את הגדרת האתגר עצמו ע"י כך שנימנע לחלוטין מהעברת נתונים סודיים של הקונה דרך תמסורת הקול.

בעבודה המסכמת הצגנו פתרונות קודמים לפתרון זה אשר גם הם פתרונות מאסכולת ההצפנה. פתרונות אלו התמקדו בהעברה של נתון סודי (נניח- מספר כרטיס אשראי) בין מכשיר המוכר לבין מכשיר הקונה. הסתמן כי די בשליחתו של נתון סודי בין שני רכיבים אשר לא קיימת ביניהם כל היכרות מוקדמת בכדי להפוך את הפתרון לחדיר למתקפה מסוג 'אדם באמצע'. מתקפה המאפשרת להשיג את הנתון הסודי הנשלח.

השכלול בפתרון זה הוא שבמקום להשתמש בנתון סודי של מספר כרטיס אשראי אנו נשתמש במזהה חח"ע של הקונה, אשר איננו יוגדר עוד כסודי. נתאר פרוטוקול בו השגתו של המזהה ע"י תוקף לא אמורה להיות מספיקה בשביל להתחזות לקונה.

הפתרון המפורט בפרק זה הינו רעיון מקורי של המחבר.

בפתרון זה מפעילת השירות תפעיל שרת קצה אשר יגלם יכולת של CA (Certificate Authority) כפי שמתואר בתקן X.501 [2], אשר ינפיק עבור כל לקוח תעודה דיגיטלית (Certificate). כמו כן, השרת גם יאחסן באופן מרוכז את התעודות דיגיטליות של כלל הלקוחות המשתמשים בשירות.

הכנה מקדימה (בעת ההגדרה הראשונית/אחת לתקופה)-

- כל מכשיר קונה, אשר עליו מותקנת האפליקציה של שירות התשלומים, בעת ההרשמה לשירות ינפיק זוג מפתחות אסימטרים, פרטי וציבורי. המפתח הפרטי יישמר במכשיר הקונה, בעוד המפתח הציבורי יישלח לשרת הקצה באמצעות הודעת CSR (Certificate Signing Request).
- התקשורת בין האפליקציה לבין שרת הקצה תתבצע באופן מוצפן ומאובטח ע"י המשתמש והסיסמא של הקונה אשר הונפקו לו מבעוד מועד כאשר נרשם לשירות.
- שרת הקצה ינפיק מזהה חח"ע עבור אותו לקוח. מזהה זה לא יוגדר כסודי (כמו לדוגמא מספר כרטיס אשראי).
- כתגובה להודעת הCSR, שרת הקצה יחזיר למכשיר הקונה תעודה דיגיטלית, כפי שמתואר בתקן X.501, אשר יכיל את המפתח הפומבי של הלקוח יחד עם המזהה החח"ע של הלקוח. התעודה הדיגיטלית תהיה חתומה ע"י CA שיופעל בצד של שרת הקצה ע"י מפעילת השירות, ה-CA יחתום על התעודה הדיגיטלית בעזרת מפתח פרטי פנימי ובכך יעיד על אמינותה.
- התעודה הדיגיטלית תהיה בתוקף לזמן מוגבל. אחת לתקופה אפליקציית הקונה תנפיק זוג מפתחות אסימטריים חדשים ותתחבר לשרת הקצה של ספק השירות על-מנת שיחתום באמצעות שרת ה-CA על המפתח הציבורי החדש בכדי לייצר תעודה דיגיטלית חדשה. התעודה הדיגיטלית החדשה תכיל

מזהה קונה חדש אשר יונפק ע״י נותן השירות, ואילו המזהה הישן יסומן בשרת הקצה כחסום לשימוש.

- אצל כל מכשיר מוכר יוגדר מראש שרת ה-CA הנ״ל כאחד משרתי ה-CA שהוא סומך עליהם.

בעת הקניה הפרוטוקול יעבוד בצורה הבאה

- לאחר שהקונה יראה את מחיר העסקה על מסך המוכר הוא ילחץ על כפתור התחלת עסקה במכשיר הקונה.
- מכשיר הקונה ימיר את המזהה החח״ע של הקונה לקול וישדר אותו באמצעות תמסורת קול לעבר מכשיר המוכר, כאשר בתחילת אותו מסר ישורשר צליל התחלת עסקה.
- מכשיר המוכר יפענח את השדר וישדר את המזהה החח״ע המפוענח של הקונה לשרת הקצה יחד עם מחיר העסקה ע״מ לוודא כי העסקה יכולה להתבצע.
- במידה ומדובר במזהה של לקוח קיים ובמידה שברשותו מספיק יתרה במסגרת האשראי, שרת הקצה ישלח את התעודה הדיגיטלית של הקונה למכשיר המוכר. מכשיר המוכר יוודא כי התעודה הדיגיטלית אכן מכילה את המזהה החח״ע של אותו קונה.
- מכשיר המוכר ישתמש במפתח הפומבי של הקונה הממוקם בתוך התעודה הדיגיטלית ע״מ להצפין מחרוזת אתגר אקראית יחד עם מחיר העסקה, שם בית העסק ומספר התשלומים המקסימלי האפשרי. מכשיר המוכר ימיר את המסר המוצפן לתמסורת קול וישדר אותו לעבר הקונה.
- מכשיר הקונה יקלוט את המסר, יפענח אותו באמצעות המפתח הפרטי, יציג לקונה על המסך את המחיר, שם בית העסק, יבקש ממנו לבחור את מספר תשלומים הרצוי (בחירה מתוך רשימה נגללת) ויבקש אישור (בדמות לחיצה של הקונה על כפתור) לבצע את העסקה.
- במידה והקונה אישר את העסקה, מכשיר הקונה יקודד את מסר האתגר האקראי המפוענח (אשר הגיע מוצפן ממכשיר המוכר), את האישור לביצוע העסקה ואת מספר התשלומים הנבחר על גבי תמסורת קול, וישדר אותם לעבר מכשיר המוכר.
- מכשיר המוכר יוודא כי המסר הרנדומלי אשר קיבל זהה למסר המקורי אשר שלח לעבר מכשיר הקונה.
- או אז, מכשיר המוכר ישלח לשרת הקצה הודעה על בקשה לביצוע עסקה שתכלול את מזהה הקונה, המחיר ואת מספר התשלומים הנבחר ע״י הקונה.
- שרת הקצה יחזיר למכשיר המוכר הודעת אישור על כי העסקה התבצעה.
- מכשיר המוכר יציג על צג המוכר חיווי על אישור ביצוע העסקה.

איך מתבצע Revocation

במקרה בו הקונה מאמין כי המפתח הפרטי שלו נחשף, הוא יצטרך להנפיק באופן יזום ובאמצעות האפליקציה שמותקנת על מכשירו, זוג מפתחות חדש (כפי שממילא מתבצע אחת לתקופה). שרת הקצה ינפיק עבור מכשיר הקונה תעודה דיגיטלית חדשה אשר תכיל את המפתח הפומבי החדש ומזהה קונה חדש. מזהה הקונה הישן יסומן ע״י שרת הקצה כחסום לשימוש.

מכיוון שבחרנו בדרך פעולה זו, אין צורך להשתמש במנגנון של CRL (Certificate Revocation List) המתואר בתקן X.509. שימוש במנגנון זה היה מחייב את ספק השירות להעביר באופן שותף לכל(!) מכשירי המוכרים רשימה של מספרים מזהים של כל התעודות הדיגיטליות אשר הוגדרו כ-Revoked. מכשיר המוכר היה נאלץ לעבור על כל הרשימה עבור כל עסקה בכדי לוודא שהמספר הסידורי של התעודה הדיגיטלית שקיבל ממכשיר הקונה אינו נמצא ברשימה. בחירה בשימוש ברשימת CRL היה מחייב אותנו, בכל פעם שקונה כלשהו מחליף תעודה, להפיץ את הרשימה לכלל מכשירי המוכרים, דבר שהיה מסרבל את הפתרון.

אפשר להיווכח כי צורת עבודה זו מהווה חריגה מהשימוש הקלאסי בX.509, אשר מתאר את תהליך האימות בין שתי ישויות ברשת מסוימת באמצעות אימות התעודה הדיגיטלית שעברה בין ישות אחת לשניה אל מול רשימת של CAים קבועה. בפתרון זה לעומת זאת, הקשר המאובטח שקיים ממילא בין מכשיר המוכר לשרת הקצה מנוצל בכדי למשוך את התעודה הדיגיטלית המעודכנת של הקונה משרת הקצה בכל עסקה.

אומנם כאשר ישות א׳ רוצה לאמת את זהותה של ישות ב׳, לא נהוג שגורם שלישי מעביר לצורך כך תעודה דיגיטלית למטרת השוואה, אולם, עצם העובדה שעבור מכשיר מוכר, סביר להניח שבדר״כ עסקה מתבצעת אחת למספר דקות, ניכר שניתן להשתמש בדרך פעולה זו ללא השלכות של ביצועים. זאת בניגוד לתקשורת SSL סטנדרטית לדוגמא, שבה הנחה כזו לא יכלה לתפוס (רכיב תקשורת בתשדורת SSL עלול להידרש לוודא תעודות דיגיטליות גם מספר פעמים בשניה).

נגדיר מספר סימונים, כמו כן, נגדיר את מספר הסיביות של כל מסר למעט אלו שאינם עוברים באופן גולמי באמצעות תמסורת הקול-

סימון	מספר תווים	תיאור
Ctrkey	**-**	**התעודה הדיגיטלית המבוססת על המפתח הפומבי key**
Rand	8	המחרוזת הרנדומלית
BuyerPubKey	**-**	**המפתח הפומבי של הקונה**
BuyerPrvKey	-	המפתח הפרטי של הקונה
EncBuyerPubKey(M)	**44**	**פונק' ההצפנה של הודעה M באמצעות המפתח הפומבי של הקונה**
DecBuyerPrvKey(M)	-	פונק' הפענוח של הודעה M באמצעות המפתח הפרטי של הקונה
EncryptLength	**3**	**אורכו בבסיס הקסדצימלי של המסר המוצפן לעיל. המסר המוצפן ישודר מיד לאחר שידור אורכו**

נתאר באמצעות טבלה את מהלך מעבר הנתונים בפרוטוקול-

Function	**יעד**	**מקור**
V(TransPrice, BusinName, MaxPmt)	מסך מוכר	מכשיר מוכר
S_1(BuyerId)	מכשיר מוכר	מכשיר קונה
$N_{seller/get\text{-}buyer\text{-}certificate}$(SellerUser, SellerPassword, BuyerId)	שרת הקצה	מכשיר מוכר
N($Ctr_{BuyerPubKey}$)	מכשיר מוכר	שרת הקצה
S_2(EncryptLength, $Enc_{BuyerPubKey}$(TransPrice, BusinName, MaxPmt, Rand))	מכשיר קונה	מכשיר מוכר
P(TransPrice, BusinName, MaxPmt)	צג קונה	מכשיר קונה
S_3(BuyerConfirmation, ChosenPmt, Rand)	מכשיר מוכר	מכשיר קונה
$N_{seller/get\text{-}server\text{-}confirmation}$(SellerUser, SellerPassword, BuyerId, TransPrice, ChosenPmt)	שרת הקצה	מכשיר מוכר
N(ServerConfirmation)	מכשיר מוכר	שרת הקצה
V(ServerConfirmation)	מסך מוכר	מכשיר מוכר

4.2. פתרון Time-based One-time Password משולב עם גיבוב מידע

בעבודה המסכמת הוסבר כי הצפנה אסימטרית אומנם יכולה להעניק הגנה טובה ממתקפות אדם-באמצע, אולם מפאת התקורה שהיא מוסיפה למסר הקול הנשלח, יתכן כי לא ניתן יהיה להשתמש בה עבור פתרונות ארנק דיגיטלי מבוססי קול.

כפי שנאמר מקודם, הצפנה סימטרית לבדה איננה אפשרית, מכיוון שאין דרך בטוחה לבצע את העברת המפתח בין הצדדים (מתוך ההנחה שכל עסקה חייבת להיות חסרת תכנון מקדים).

אם כן, נרצה לאתר פתרון אחר אשר מוגן ממתקפת אדם באמצע, אך ללא כל שימוש בהצפנה.

הפתרון המפורט בפרק זה הינו רעיון מקורי של המחבר עם השראה הלקוחה משילוב של פתרונות [3] ו-[4].

חברת Edgetech Solutions המספקת פתרונות לבנקים וממוקמת בזימבאבואה, השיקה אפליקציית מובייל בשם :EdgePay app. החברה פיתחה פתרון מסקרן למימוש ארנק דיגיטלי מבוסס תמסורת קול, המשלב שימוש ב-Time-based One-time Password Algorithm [3].

Time-based One-time Password Algorithm (או בקיצור TOTP) – הוא אלגוריתם, המתואר בפירוט בתקן RFC 6238 [4], המייצר token חד-פעמי מהיתוך של מחרוזת סודית ארוכה וקבועה, יחד עם הזמן הנוכחי. האלגוריתם משתמש בפונקציית גיבוב (Hash) קריפטוגרפית על-מנת לייצר token בעל אורך קצר, אשר מתחלף מדי מספר שניות (לרוב מדובר באינטרוולים של 30 שניות/דקה).

אחד מהשימושים הנפוצים בTOTP הוא לצורך אימות זהות דו-שלבי (two factor authentication) של משתמש. באופן זה הtoken הזמני משמש כאמצעי אימות הכרחי בדף אימות זהות, בנוסף להזנה של סיסמה קבועה. באופן מעשי, המשתמש מייצר את ה-token באמצעות חומרה ייעודית (בד"כ בגודל של מחזיק מפתחות) שעליה מסך קטן. המחרוזת הסודית נצרבה בתוך החומרה מבעוד מועד. מדי מסגרת זמן, החומרה מציגה על המסך את ערך ה-token הנוכחי באמצעות ביצוע פונקציית גיבוב בין המחרוזת הקבועה לבין הזמן הנוכחי אשר מתקבל מרכיב שעון פנימי אשר ממוקם במכשיר. לחילופין, במקום להשתמש בחומרה ייעודית, ניתן גם לעשות שימוש בטלפון חכם אשר מסוגל לבצע פונקציונאליות דומה.

אופן השימוש ב-TOTP לצורך אימות זהות של משתמש אל מול שרת הוא כדלקמן-

- לאחר שהמשתמש הזין במסך ההזדהות שמולו את הסיסמא הקבועה שלו, עליו להזין גם שדה שני (מכאן- נובעת ההגדרה 'אימות זהות דו-שלבי'), זהו ה-token הרלוונטי לחלון הזמן הספציפי הנוכחי. את ה-token המשתמש מעתיק מצג החומרה שברשותו או מהאפליקציה.
- השרת מקבל את הסיסמא ואת ה-token מהמשתמש, מנסה לייצר token בעצמו ומוודא האם שני ה-token-ים הם זהים. רק במידה והם זהים (והסיסמא תקינה) השרת יסכים לאשר את ההתחברות של אותו משתמש.

התפיסה מאחורי השימוש ב-TOTP לצרכי אימות זהות היא שגם המשתמש וגם צד השרת מחזיקים ברשותם:

1. את המחרוזת הסודית הקבועה.
2. את אלגוריתם הפעולה של פונקציית הגיבוב.
3. את הזמן הנוכחי (במילים אחרות- השעונים של הלקוח ושל השרת צריכים להיות מסונכרנים ביניהם).

נשים לב כי היחידים שאמורים להחזיק את אותה מחרוזת סודית אמורים להיות אך ורק הלקוח והשרת והיא אינה אמורה להיחשף בשום שלב לשום גורם שלישי.

אלגוריתם הפעולה של פונק' הגיבוב הוא אינו בהכרח סודי, אך זהו אינו תמיד המקרה. לדוגמא עבור סוג מימוש TOTP המכונה SecurID [5] אשר פותח ע"י RSA, חטיבת המחקר של חברת EMC, החברה מסרבת באדיקות לחשוף מהי פונק' הגיבוב המדויקת בה הם משתמשים. חרף עובדה זאת, החברה הודיעה כי האבטחה של המוצר אינה תלויה בשום אופן בהישארות של האלגוריתם כסודי. נעשו ניסיונות ע"י מספר גורמים לבצע 'הנדסה לאחור' ע"מ לשחזר את אותה פונק' גיבוב. ישנו מאמר בנושא [6] אשר כותבו טוען כי הוא הצליח בכך ואף פירט אותו במאמר.

הכוח האבטחתי ב-TOTP נובע בעיקר מהצורה שבה הורכב ה-token. בניגוד למחרוזת המקורית, ה-token עצמו איננו נחשב כסודי ולכן ניתן להעבירו ללא חשש דרך תווך מסוים שאיננו מאובטח. מכיוון שה-token מורכב בין השאר גם מהזמן הנוכחי, נובע מכך שגם אם יצליח תוקף להעתיק את ה-token העכשוי, ה-token ממילא יהפוך לחסר ערך עבורו בסיום אותו חלון הזמן. מלבד זאת, מתוך השימוש בפונקציית גיבוב נובע כי במידה ותוקף יצליח לשים ידיו על ה-token, הוא אינו אמור להצליח לשחזר את המחרוזת הסודית. הסיבה לכך היא שפונקציית הגיבוב היא חד כיוונית לחלוטין וכאשר הפכה את המחרוזת הארוכה ל-token קצר, אבד בדרך רוב המידע על אותה המחרוזת. גם אם ברשותו של התוקף tokenים רבים אשר נגזרו מאותה מחרוזת סודית (מחלונות זמן שונים), ובמידה ואנו משתמשים בפונק' גיבוב איכותית, התוקף לא אמור להצליח לשחזר את המחרוזת הסודית. בנוסף לכך, פונק' הגיבוב גם מבטיחה כי התוקף לא יוכל להסיק מ-token של חלון זמן מסוים את ה-token של חלון הזמן הבא אחריו (או כל חלון זמן אחר לצורך העניין).

מכיוון שהתיעוד על הפתרון של EdgePay הוא עדיין דל יחסית מכיוון שהמוצר טרם יצא לשוק, נרשה לעצמנו לבצע הנחות לגבי הפתרון בכדי להתאים לתהליך מהלך העסקה הבסיסי אשר תיארנו מקודם. הרעיון המרכזי בפתרון שנתאר להלן הוא שבכל מסר שישלח על גבי תמסורת קול אנו נקפיד לצרף token למסר הנשלח.

הזכרנו בעבודה המסכמת גם כן את הבקשה לפטנט אשר הוגשה לרשם הפטנטים מטעם **Bank of America** [7]. בקשה זו מתארת פתרון לארנק דיגיטלי מבוסס תמסורת קול (אשר אינו דורש תקשורת לשרת הקצה בזמן ביצוע העסקה). אחת מהתכונות של הפתרון הוא השימוש בשליחה של token בשלב אישור העסקה ע״י הקונה ממכשיר הקונה למכשיר המוכר, זאת על מנת לאמת שאכן הקונה הוא זה שאישר את העסקה. ה-token נבנה ע״י אלגוריתם מסוים אשר אינו נחשף במסגרת הפטנט (אך סביר להניח שמדובר באלגוריתם גיבוב מסוג כלשהו), אשר יוצר אותו כתלות בזהות חשבון החיוב של הקונה ובמחיר של העסקה. במילים אחרות, בפתרון זה ה-token למעשה נגזר גם מחלק מנתוני העסקה (במקרה זה, ממחיר העסקה), ובאופן זה עוזר למנוע שימוש ב-token ע״י תוקף עבור עסקה אחרת (אשר ההנחה היא כי רוב הסיכויים שהמחיר בה יהיה שונה) ע״מ להתחזות לקונה ולחייב על חשבונו.

הכנה מקדימה (בעת ההגדרה הראשונית)

- מכשיר הקונה ישלח לשרת הקצה את המזהה החומרתי החח״ע (חד-חד ערכי) של מכשיר הטלפון החכם של הקונה שהוטבע בחומרת המכשיר ע״י היצרן. שרת הקצה ישמור מעתה את אותו מזהה ברשומת מסד הנתונים שלו עבור הקונה.
- ספק השירות ינפיק לקונה 3 קודים סריאליים אקראיים (לצורך הדוגמא- בני 12 ספרות דצימליות כל אחד), אשר ייוחסו מעתה ע״י שרת הקצה באופן חד-חד-ערכי למכשיר הקונה, אותן הקונה יצטרך להזין באופן חד פעמי לאפליקציית השירות המותקנת במכשיר. ספק השירות ישמור את שלושת הקודים הסריאליים גם הוא. **קודים אלו נחשבים סודיים ופרטיים** ומהם, ובשילוב עם המזהה החומרתי של מכשיר הטלפון החכם, יגזרו שלושת ה-token-ים שישמשו לזיהוי בין מכשיר הקונה למכשיר המוכר. מובן כי במידה ותוקף יצליח לשים את ידיו על מזהים אלו אותו תוקף יוכל להתחזות לקונה.
- כמו כן, ספק השירות ינפיק מזהה חח״ע נוסף לקונה. מזהה זה איננו יחשב בגדר נתון סודי, וניתן יהיה לשלוח אותו ללא הצפנה בין מכשיר הקונה לבין מכשיר המוכר.
- הקונה צריך לוודא כי השעה במכשיר שלו מעודכנת.

אופן הנפקת ה-token

- נעשה שימוש בפונק׳ גיבוב המיועדת לאלגוריתם מסוג TOTP.
- אינטרוול הזמן שיוגדר כקלט לפונק׳ הגיבוב לצורך יצירת ה-token יוגדר לעבוד בקבועים מסוימים (נניח של 60 שניות).
- פונק׳ הגיבוב תקבל כקלט את הקוד הסריאלי הרלוונטי לאותו שלב בפרוטוקול, את המזהה החומרתי של הטלפון החכם של הקונה ואת חלון הזמן הנוכחי.

בעת הקניה הפרוטוקול יעבוד בצורה הבאה

- לאחר שהקונה יראה את מחיר העסקה על מסך המוכר הוא ילחץ על כפתור התחלת עסקה במכשיר הקונה.
- מכשיר הקונה ינפיק את token1 כנגזרת של פונקציית הגיבוב על הקוד הסריאלי הראשון, על מזהה החומרה של המכשיר ועל הזמן הנוכחי.
- מכשיר הקונה ישלח את רצף צלילי התחלת עסקה ובצמידות אליו את המזהה החח״ע של הקונה ואת token1 באמצעות צלילים.
- מכשיר המוכר יקבל את מזהה הקונה ואת token1 וישדר אותם יחד עם מחיר העסקה, שם בית העסק ומספר התשלומים המקסימלי לשרת הקצה.
- שרת הקצה יוודא את תקינות מזהה הקונה ויבדוק אם העסקה יכולה להתבצע בהתחשב במסגרת האשראי של אותו קונה.
- כמו כן, שרת הקצה ינפיק token על בסיס הקוד הסריאלי הראשון של הקונה. על מזהה החומרה של המכשיר ועל הזמן הנוכחי, ויוודא כי token זה זהה לאותו token1 שקיבל.
- כעת במידה והבדיקות יעברו בהצלחה, שרת הקצה ינפיק את token2 כנגזרת של פונקציית הגיבוב על הקוד הסריאלי השני, על מזהה החומרה של המכשיר, מחיר העסקה, מספר התשלומים המקסימלי האפשרי, שם בית העסק ועל הזמן הנוכחי.
- שרת הקצה יחזיר למכשיר המוכר אישור על המשך העסקה ובנוסף את token2.
- מכשיר המוכר ישלח לעבר מכשיר הקונה באמצעות תמסורת צלילים את token2 יחד עם מחיר העסקה, מספר התשלומים המקסימלי האפשרי ושם בית העסק.
- מכשיר הקונה יקלוט את המסר, ינפיק את token2 ויוודא שהתוצר שהתקבל מפונקציית הגיבוב זהו אותו token2 שהונפק ע״י שרת הקצה.
- כעת מסך מכשיר הקונה יציג את מחיר העסקה, מספר התשלומים האפשריים ושם בית העסק. על הקונה לוודא כי שם בית העסק הוא אותו עסק שמולו הוא מבצע את הקניה, לבחור את מספר התשלומים שבהם הוא מעוניין מתוך הרשימה המוצגת ולאשר את העסקה ע״י לחיצה על כפתור.
- בשלב זה הקונה ינפיק את token3 כנגזרת של פונקציית הגיבוב על הקוד הסריאלי השלישי, על מזהה החומרה של המכשיר, מספר התשלומים שנבחרו ע״י הקונה, סטטוס אישור הקונה (קונה אישר/לא אישר את העסקה) ועל הזמן הנוכחי וישדרו בתמסורת צלילים לעבר המוכר יחד עם סטטוס אישור הקונה ואת מספר התשלומים שנבחר.
- מכשיר המוכר ישלח את token3, סטטוס אישור העסקה ואת מספר התשלומים שנבחר לעבר שרת הקצה.
- שרת הקצה ינפיק את token3 ויוודא כי זהו אותו token3 שהתקבל ממכשיר המוכר.

- במידה וכן, שרת הקצה יבצע את העסקה וישלח הודעת אישור עסקה למכשיר המוכר, אשר מצידו ישלח אישור חזותי לעבר מסך המוכר המציין כי העסקה הושלמה בהצלחה.

אופן וידוא ה-token

- כאשר אחד המכשירים יקבל את ה-token מהצד השני הוא ידאג לייצר בעצמו את אותו ה-token (ההנחה היא שלשני הצדדים ישנם הנתונים הנדרשים ע״מ לייצר את אותו ה-token) ויבצע השוואה בין התוצר שהתקבל אצלו לבין ה-token אשר יתקבל.
- מכיוון שה-token מורכב גם מהדקה הנוכחית, יתכן מצב בו בשלב הוידוא שני ה-token-ים יהיו שונים. יתכן שה-token נוצר ממש בסמוך לפקיעתו, או שפשוט עבר זמן רב מדי מהרגע שנוצר אותו ה-token ועד אשר הוא פוענח ביעד הישר מתמסורת הצלילים, כמו כן לא ניתן לפסול את האפשרות לפער זמנים קטן בין שעוני שני הרכיבים.
- מסיבה זו, כאשר ה-token-ים אינם תואמים, יתבצע ניסיון נוסף להשוות את ה-token יחד עם ה-token של הדקה הקודמת (וליתר ביטחון גם עם זאת שלפניה) וגם עם ה-token של הדקה הבאה (וליתר ביטחון גם עם זאת שאחריה). מכיוון שיצירת token היא פעולה אריתמטית מהירה, אין לנו מניעה לייצר token-ים מספר פעמים בעת וידוא.

נגדיר מספר סימונים, כמו כן, נגדיר את מספר הסיביות של כל מסר למעט אלו שאינם עוברים באופן גולמי באמצעות תמסורת הקול-

סימון	מספר תווים	תיאור
SerialCode1/2/3	**-**	**הקוד הסריאלי הראשון/שני/שלישי של הקונה.**
HwId	-	המזהה החומרתי החח״ע של הטלפון החכם של הקונה.
Token1/2/3	**6**	**הtoken הראשון/שני/שלישי שמונפק ע״י הקונה ושרת הקצה.**
CurrentTime	-	הזמן הנוכחי.
TokenHash(a,b)	**6**	**פונקציה אשר מחזירה פלט של גיבוב עבור שני פרמטרים- a ו-b.**

נתאר באמצעות טבלה את מהלך מעבר הנתונים בפרוטוקול -

מקור	יעד	Function
מכשיר מוכר	מסך מוכר	V(TransPrice, BusinName, MaxPmt)
מכשיר קונה	מכשיר מוכר	S_1(BuyerId, TokenHash(CurrentTime, HwId, SerialCode1))
מכשיר מוכר	שרת הקצה	$N_{seller/get-token2}$(SellerUser, SellerPassword, BuyerId, TransPrice, BusinName, MaxPmt, Token1)
שרת הקצה	מכשיר מוכר	N(TokenHash(CurrentTime, HwId, SerialCode2, TransPrice, BusinName, MaxPmt))
מכשיר מוכר	מכשיר קונה	S_2(TransPrice, BusinName, MaxPmt, Token2)
מכשיר קונה	צג קונה	P(TransPrice, BusinName, MaxPmt)
מכשיר קונה	מכשיר מוכר	S_3(BuyerConfirmation, ChosenPmt, TokenHash(CurrentTime, HwId, SerialCode3, ChosenPmt))
מכשיר מוכר	שרת הקצה	$N_{seller/get-server-confirmation}$(SellerUser, SellerPassword, buyerId, TransPrice, ChosenPmt, Token3)
שרת הקצה	מכשיר מוכר	N(ServerConfirmation)
מכשיר מוכר	מסך מוכר	V(ServerConfirmation)

נשים לב כי מתקיימת בפתרון זה הנחה מסוימת מצד הקונה ע״מ לשמור על העסקה מאובטחת, מכיוון כי נדרשת תשומת לב מצד הקונה בעת שלב אישור העסקה. ז״א, לפני שהקונה מחליט לאשר את העסקה, הוא צריך לשים לב כי שם בית העסק ומחיר העסקה אשר מופיעים על מסך מכשירו הם תקינים. לעניות דעתי זוהי הנחה סבירה אשר ניתן לצפות מצד הלקוח.

5. עבודה עם צלילים

5.1. אמינות התווך

בניגוד לתמסורת מבוססת על RF, לתמסורת קול אין תחום תדרים שניתן לצפות שיהיה בהם שקט מהפרעות חיצוניות. על כן, תווך הקול נחשב כבעל אמינות העברת נתונים נמוכה. מכך מובן כי בכדי להצליח לקיים תקשורת רציפה, אין מנוס מלהשתמש באמצעי לתיקון שגיאות. הפתרון המתבקש בכדי לצמצם את השפעת ההפרעות החיצוניות הוא שימוש בתוספת של שכבת סיכום ביקורת (Checksum) עבור כל מסר שנשלח.

הצד שמקבל את המסר ישתמש בסיכום הביקורת ע״מ לנסות לתקן את המסר במידה ונפגם.

במידה והמסר המתקבל מגיע ליעדו כשהוא פגום מדי מכדי לתקנו, יהיה צורך לבצע את שליחת אותו המסר מחדש. בכדי שהצד השולח יתוודע לכך שעליו לשלוח מחדש את המסר, הצד המקבל צריך להודיע לו לעשות כן, ובכדי שזה יהיה אפשרי יש להוסיף הודעות אישור קבלה (Acknowledge) לפרוטוקול העסקה. הבעיה היא שתוספת כזו לפרוטוקול תוסיף תקורה נוספת על תווך שמפאת האמינות הנמוכה שלו אנו משתדלים להעביר דרכו מעט מידע ככל האפשר.

על כן, נניח כי במקרה של כישלון בפענוח המסר, הקונה יאלץ ליזום התחלה מחדש של תהליך העסקה.

נציין כי החיסרון של השימוש בסיכום ביקורת היא התקורה ששכבה זו מוסיפה לגודלו של המסר הנשלח. בסוג תמסורת עם אמינות נמוכה כגון זו, נאלץ להוסיף למסר שכבת סיכום ביקורת גדולה ביותר. בשל כך, מהירות השליחה בפועל של המסר הגולמי תהיה נמוכה יותר כאשר מצרפים למסר את שכבה זו.

נשאף להעביר כמות נמוכה ככל שאפשר של נתונים באמצעות תווך הקול. ז״א, ננסה להעביר בין הצדדים בעסקה רק מה שבאמת רלוונטי למען ביצוע העסקה. כל נתון עודף מעלה את הסיכוי לשגיאות, כמו גם מעלה את זמן השליחה של מסר הקול.

ע״מ לצמצם את הסיכוי לשגיאות, נשתדל גם בעת ששני המכשירים ׳משוחחים׳ ביניהם, להציבם קרוב ככל שאפשר אחד לשני בכדי שהמסר יעבור בצורה ברורה יותר. אם מתאפשר, ננסה גם לדאוג ל׳הפרדה אקוסטית׳ בין שני המכשירים לבין העולם (לדוגמא, באמצעות הצבת מכשיר הקונה עצמו יחד עם המיקרופון של מכשיר המוכר בתוך תא זכוכית קטן אטום לרעשים).

5.2. תחום השימוש בצלילים

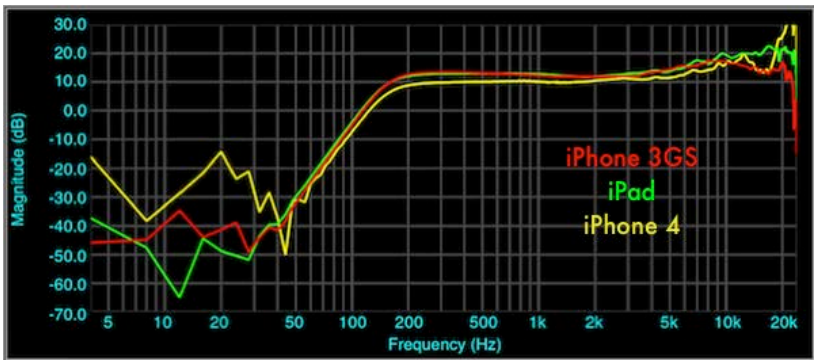
מתוך העובדה שאנו עושים שימוש בתווך קול, יכולות להיות השלכות מעניינות בבחירתנו לגבי אילו צלילים יבחרו ע״מ להרכיב את הא׳-ב׳ של התמסורת.

ישנם פתרונות לארנק דיגיטלי (כגון Way2ride אשר נזכיר אותו בפרק הבא) אשר מתבססים על שימוש במרחב צלילים אולטראסוני בכדי להעביר מידע בין מכשיר המוכר למכשיר הקונה.

קול אולטראסוני הוא קול המשודר בתדירות גבוהה מזו שאדם יכול לשמוע, ולכן יתרונו הבולט הוא שאינו מהווה הפרעה לאוזן האנושית. מכיוון שתחום השמע של האדם הוא בין התדרים 20Hz ועד 20kHz בקירוב (כאשר תחום התדרים העליון נפגע במהלך השנים ויכול לרדת עד ל-16kHz בקירוב. ז״א ילדים מסוגלים לשמוע תדרים שמבוגרים כבר אינם שומעים), שידור צליל בתדר גבוה מ-20kHz יגרום לכך שרוב מוחלט של בני האדם לא יהיו מסוגלים לשמוע אותו.

יתרון נוסף הוא שמכיוון שצלילים אולטראסונים מטבעם אינם כה נפוצים במרחב האורבני, לשימוש בהם ישנו פוטנציאל להפחית את הסבירות להפרעות בשעת ביצוע העסקה.

אך החיסרון המשמעותי בשימוש בסוג צלילים זה הוא מרחב התדרים הריאלי שניתן להשתמש בו. בזמן שרכיב הרמקול של טלפון חכם מסוגל לשדר עמוק בתחום התדרים האולטאסוניים, המיקרופון של טלפון חכם סטנדרטי מסוגל לרוב לתמוך מעט מעל תדר 20kHz [8]. כפי שניתן לראות באיור 1 להלן [8] המתאר את ההתבדרות הנוצרת באיזור תדר זה עבור טלפונים חכמים מסוג iPhone-



-איור 1

האיור מציג גרף המתאר עבור כל תדר (ציר ה-x) את ערך ה-Frequency Response ביחידות של דציבלים עבור אותו מכשיר (ציר ה-y). במילים אחרות, מציג עבור כל מכשיר את מידת הדיוק שלו בכל תדר. ניתן לראות בגרף כי בערך בסביבות התדר 20khz (שהוא בדר״כ גם התדר המקסימלי הנקלט ע״י האוזן האנושית) מידת הדיוק מתחילה להתבדר. ז״א- זהו התדר המקסימלי הריאלי עבור המכשירים המתוארים.

ז״א, ברוב הטלפונים לא נותר מרחב תדרי קול אולטראסוני רחב דיו שבו ניתן להשתמש. במילים אחרות, הא׳-ב׳ של סוגי הצלילים השונים יהיה קטן יחסית ובשל כך, קצב שידור המידע בין מכשיר הקונה למכשיר המוכר יהיה נמוך יותר כאשר משתמשים במרחב צלילים אולטראסוני בעת ביצוע עסקה ע״י שימוש בטלפון חכם.

מנגד, ישנם מימושים של הטכנולוגיה אשר מאמצים בברכה צלילים הנשמעים ע״י האוזן האנושית.

דוגמא טובה לכך היא האפליקציה לטלפונים חכמים הנקראת Chirp [9] אשר פותחה ע״י חוקרים מאוניברסיטת לונדון ומשתמשות ברצף צליליים המדמים ציוץ של ציפורים בכדי להעביר מידע בין שני מכשירי טלפון חכם. האפליקציה פועלת באופן הבא-

נניח כי המטרה היא להעביר קובץ (למשל תמונה) בין שני טלפונים חכמים אשר בעליהם הם אליס ובוב (שנמצאים שניהם בסמיכות) ועליהם מותקנת האפליקציה. באמצעות האפליקציה אליס בוחרת את קובץ התמונה במכשירה. הקובץ מועלה דרך הרשת הסלולארית ממכשירה של אליס לעבר שרת צד שלישי מאובטח (ענן). על השרת בענן, הקובץ מקוטלג ע״י מספר מייצג חד-חד ערכי. המספר נשלח לטלפון החכם של אליס,

והאפליקציה על הטלפון של אליס ממירה את המספר באופן חח״ע (חד-חד ערכי) ע״י אלגוריתם ידוע לקבוצת צלילים אשר מדמים קולות ציפורים אשר משודרים דרך הרמקול של המכשיר של אליס לעבר חלל האוויר. על מכשירו של בוב, האפליקציה אשר רצה בmode של האזנה, מבחינה ברצף הצלילים, מקליטה אותם וממירה אותם בחזרה למספר המקורי. ממכשירו של בוב, המספר נשלח לעבר השרת בענן. השרת שולח למכשירו של בוב את הקובץ אשר תואם למספר זה.

בכל אופן, לצורך הקלת הדגמת הרעיון, אנו נתמקד בשיטת המרה חח״ע בין צליל לבין תו. ז״א, עבור כל תו באי-בי ממנו מורכבים המסרים אנו מעוניינים להעביר, נקצה צליל יחיד ויעודי ממרחב הצלילים הנבחר. מובן כי לעיתים ניתן לבחור צורת מימוש אשר ממפה רצף של תווים (יותר מתו בודד) לצליל יחיד. צורת מימש שכזו תאיץ את זמן שליחת המסר, אך באותו זמן תדרוש שימוש במרחבי צלילים גדולים יותר.

נושא שכדאי לציין הוא כי קיימות מגבלות פיסיקליות שונות על יכולת הקליטה של המכשיר המקבל את המסר. אחת ממגבלות אלו, היא הצורך בקיום הפרש מינימלי מסוים בין שני תדרי צלילים סמוכים ע״מ שהמסר ייקלט כהלכה. ערכו של הפרש זה יכול להיות שונה עבור מכשירים מיצרנים או דגמים שונים (תלוי בין השאר בטיב המיקרופון ובמהירות הדגימה). ז״א, בכדי שהפתרון ייתמך במנעד רחב של דגמי מכשירים עלינו לבחור מלכתחילה בערך הפרש תדרים גבוה באופן מספק. מצד שני לא נרצה לבחור בערך גבוה מדי בכדי שלא לגרום להקטנה לא נחוצה של מספר הצלילים המאופשרים לשימוש במרחב התדרים.

נדגיש כי במסגרת עבודה זו, לא נתעמק יתר על המידה על אופן קידוד וייצוג המידע באמצעות תמסורת הקול ברובד הפיסיקלי, אלא רק כפי שנדרש ע״מ לנתח את טיב הפתרונות שיוצגו בהמשך.

5.3. הקשר שבין תו לצליל

ישנן שיטות מגוונות לצורך קידוד מסרים על גבי רצפים של צלילים. לצורך הקלת הדגמת הרעיון, אנו נתמקד בשיטת המרה חח״ע (חד-חד ערכית) בין צליל לבין תו. ז״א, עבור כל תו באי-בי ממנו מורכבים המסרים אנו מעוניינים להעביר, נקצה צליל יחיד ויעודי ממרחב הצלילים הנבחר. מובן כי לעיתים ניתן לבחור צורת מימוש אשר ממפה רצף של תווים (יותר מתו בודד) לצליל יחיד. צורת מימש שכזו תאיץ את זמן שליחת המסר, אך באותו זמן תדרוש שימוש במרחבי צלילים גדולים יותר.

נושא שכדאי לציין הוא כי קיימות מגבלות פיסיקליות שונות על יכולת הקליטה של המכשיר המקבל את המסר. אחת ממגבלות אלו, היא הצורך בקיום הפרש מינימלי מסוים בין שני תדרי צלילים סמוכים ע״מ שהמסר יקלט כהלכה. ערכו של הפרש זה יכול להיות שונה עבור מכשירים מיצרנים או דגמים שונים (תלוי בין השאר בטיב המיקרופון ובמהירות הדגימה). ז״א, בכדי שהפתרון ייתמך במנעד רחב של דגמי מכשירים עלינו

לבחור מלכתחילה בערך הפרש תדרים גבוה באופן מספק. מצד שני לא נרצה לבחור בערך גבוה מדי בכדי שלא לגרום להקטנה לא נחוצה של מספר הצלילים המאופשרים לשימוש במרחב התדרים.

אם כך במימוש הפרויקט נבחר לעבוד באופן הבא-

- נבנה מרחב אלפבית המורכבת מ68 תווים.
- השפה תכלול את התווים-
  - כחלק מהפרוטוקול נרצה להעביר מפתח פומבי אשר מיוצג כמידע בינארי גולמי. ע״מ לעשות זאת אנו נרצה לבצע שימוש בקידוד אשר ממיר מידע בינארי לתווי ASCII. הקידוד בו נעשה שימוש הוא Base64. קידוד זה מורכב מ64 תווים שונים שאותם נצטרך להוסיף לאלפבית שלנו. תווים אלו הם-
    - ‘A’-‘Z’
    - ‘a’-‘z’
    - ‘0’-‘9’
    - ‘+’
    - ‘/’
  - כמו כן, מכיוון שנרצה להעביר גם מסרים קריאים למשתמש (שם בית העסק לדוגמא), נוסיף לאלפבית גם את התווים הבאים-
    - ‘-’
    - רווח
    - ‘)’
    - ‘(’

אנו נרצה לייצג את כלל תווי האלפבית באמצעות צלילים. לשם מטרה זו, נקצה את תחום תדרי הקול -300_{HZ} 1975_{HZ}.

הפרש 25_{HZ} בין כל שני תדרים המייצגים תו הוא אופטימלי ע״מ להקטין את הסיכון בשיבוש, לכן נשתמש בהפרש זה (נסביר עוד לגבי איך הגענו למספר בהמשך).

להלן טבלה המסכמת את ההמרה החח״ע שבין תדר צליל לבין תו מיוצג-

תדר/טווח תדרים	תו מיוצג/תווים מיוצגים	כמות צלילים
300	’(‘	1 ♪x
325	‘)‘	1 ♪x
350-575	‘0’-‘9’	10 ♪x
600	רווח	1 ♪x
625	‘/’	1 ♪x
650	’+‘	1 ♪x
675	‘-‘	1 ♪x
700-1325	‘a’-‘z’	26 ♪x
1350-1975	‘A’-‘Z’	26 ♪x

5.4. צלילי שלבים

מכיוון שלא קיימת כל תקינה לגבי פרוטוקולים בהם אין הנחת חיבור בין מכשיר הקונה לשרת הקצה, בכדי לאפיין מהלך עסקה בסיסי, נתבסס על סקירת הפתרונות מסוג זה הקיימים כיום בשוק.

על כן, למען הפשטת הדברים, נניח כי פרוטוקולים בהם אין הנחת חיבור בין מכשיר הקונה לשרת הקצה, תמיד יורכבו משלושת שדרי קול הבאים-

א. שדר קולי א׳- (מסומן כS_1) נשלח בערוץ מכשיר הקונה -> מכשיר המוכר
- מטרתו העיקרית היא שידור רצון לתחילת עסקה העסקה ע״י הקונה מתוך התפיסה היא שהקונה הוא תמיד הצד המתחיל את העסקה.
- שדר זה יכול להכיל בנוסף את מזהה הקונה, או להיות ריק ממידע. במקרה שהשדר ריק ממידע תפקידו הוא רק ורק לציין את מוכנות הקונה להתחלת עסקה.

ב. שדר קולי ב׳- (מסומן כS_2) נשלח בערוץ מכשיר המוכר -> מכשיר הקונה
- מטרתו העיקרית היא לצורך שליחת שלישיית נתוני העסקה ע״י מכשיר מוכר
  - מחיר
  - כמות תשלומים אפשרית
  - שם בית העסק
- כמו כן, המוכר יכול להשתמש בשדר זה ע״מ להעביר לקונה מסר עזר נוסף אשר יהיה מיועד לשימוש מכשיר הקונה בכדי להוסיף לאבטחת העסקה (העברת מחרוזת אתגר מוצפנת, העברת מפתח פומבי וכו’).

ג. שדר קולי ג׳- (מסומן כS_3) נשלח בערוץ מכשיר הקונה -> מכשיר המוכר

- מטרתו העיקרית היא אישור של הקונה לעסקה והעברת מספר התשלומים הנבחר לעבר מכשיר המוכר.
- נציין כי ישנה אפשרות בשלב זה לשלב חיוב בהזנת סיסמא קבועה ע״י הקונה לפני אישור העסקה. שימוש בסיסמא יכול למנוע מקרים של התחזות לקונה כאשר מכשיר הקונה נגנב.
- לאחר שמכשיר המוכר מקבל את נתונים אלו הוא אמור לפנות לשרת הקצה ולאשר מולו את העסקה. במידה ושרת הקצה אישר את העסקה (וגם אם לא) החיווי על כך יוצג על גבי צג המוכר אשר ניתן לצפייה גם ע״י הקונה.

5.5. מבנה המסר הקולי

נגדיר כי כל מסר קולי משודר יהיה מורכב מהשדות הבאים-

♪x1	♪x1	♪...♪	♪x1	♪x1
צליל סיום	בדיקת סיכום ביקורת	ההודעה	צליל שלב	צליל התחלה

א. צלילי התחלה וסיום-

נקצה את התדרים אשר הקצנו עבור שידור התווים י)׳, י(׳, ז״א התדרים 325_{HZ}, 300_{HZ} בהתאמה, גם עבור שידור צלילי ההתחלה והסיום של כל שדר קולי הנשלח. נוסיף את תדרים אלו לטבלת ההמרה בין תווים לתדרים אשר הוצגה לעיל-

תדר/טווח תדרים	תו מיוצג/תווים מיוצגים	כמות צלילים
300	צליל התחלה	1 ♪x
325	צליל סיום	1 ♪x

ב. צליל שלב-

נקצה את התדרים אשר הקצנו עבור שידור המספרים 1,2,3, ז״א התדרים 425_{HZ}, 400_{HZ}, 375_{HZ}, גם עבור שידור צלילי השלבים- S_1, S_2, S_3 בהתאמה. נוסיף את תדרים אלו לטבלת ההמרה בין תווים לתדרים אשר הוצגה לעיל-

תדר/טווח תדרים	תו מיוצג/תווים מיוצגים	כמות צלילים
375-425	S_1, S_2, S_3	3 ♪x

ג. ההודעה-

ההודעה עצמה אתה אנו מעוניינים להעביר (לא כולל את שאר התקורה).

ד. בדיקת סיכום ביקורת (checksum)-

עקב בעיית אמינות התווך כפי שתוארה לעיל, עלינו להוסיף למסר הנשלח שכבה של סיכום ביקורת. נקצה לצורך כך צליל יחיד מתוך המסר הכללי אשר יבצע פונק' של סיכום ביקורת על החלק של ההודעה עצמה (מבלי לבצע על התקורה הנוספת). ניכר כי שימוש בצליל יחיד הוא מספיק בכדי לעלות בסבירות גבוהה על שיבושים במסר הנשלח ע"י הצד המקבל, אך כמובן ששימוש שכזה אינו מכיל מספיק מידע ע"מ לבצע תיקון על המידע המתקבל. במידה ובצד המקבל, לאחר השוואת ההודעה המתקבלת אל מול צליל סיכום הביקורת, נמצא כי המסר חווה שיבוש במהלך השידור, לא יהיה מנוס מלהתחיל את מהלך העסקה מהתחלה.

הפונק' שבחרנו להשתמש עבור בדיקת סיכום הביקורת היא ממוצע פשוט של תדרי המסר, אך כמובן שישנן אפשרויות רבות אחרות (כגון שימוש בפונקציית מודולו וכו').

5.6. שיטת קליטת הצליל

על מנת לקלוט את הקול הגולמי אנו נשתמש במחלקת Native של שפת Java for Android הנקראת android.media.AudioRecord. מחלקה זו מאפשרת לנו לקלוט ולנתח את הצלילים הנקלטים בזמן אמת. שימוש במחלקה לבדה אינו מאפשר לנו לפרק את המסר הקולי הנקלט למרכיבי תדרי הקול, ואנו הרי מעוניינים לבודד את מרכיבי התדרים בכדי לאתר מהו תדר הקול הדומיננטי שנשמע באותה עת. מסיבה זו נצטרך לבצע פעולה משלימה, בזמן אמת, על גבי הקול הגולמי הנקלט. הפונקציה המתמטית המאפשרת לנו להמיר קלט קול גולמי לרשימה של תדרים (נמדד בהרץ) יחד עם מרכיב עוצמת השידור (נמדד בדציבל) עבור כל תדר נקראת FFT (Fast Fourier Transform).

ישנם מספר פרמטרים אשר נדרש לקבוע כאשר המרכזיים ביותר ביניהם הם–

- קצב הדגימה- הקצב (למעשה התדר) בו המכשיר ידגום את הקול. לכל מכשיר ישנו קצב דגימה מקסימלי כתלות בחומרת המכשיר. קצב הדגימה 48,000 הוא הפופולארי ביותר במכשירי הטלפון החכם החדישים, ובו עשינו שימוש בבדיקות המימוש.
- גודל החוצץ (הbuffer)- החוצץ מתמלא מחדש בקלט הקולי בכל דגימה מחדש. גודל חוצץ קטן מדי יגרום לדיוק נמוך של המסר הנקלט. גודל חוצץ גדול מדי יגרום לעומס יתר על המעבד. אנו השתמשנו בחוצץ בגודל 4096 (גודל החוצץ חייב להיות חזקה של 2), אשר נחשב מתאים לקצב הדגימה בו נעשה שימוש.

באופן פשוט ניתן לחשב את רמת הדיוק שאנו עתידים לקבל כאשר משתמשים בפרמטרים אלו. עלינו לחלק את קצב הדגימה בגודל החוצץ, ז״א- 48000/4096=11.72. מכיוון שאנו משתמשים בהפרש של 25_{HZ} בין כל שני צלילים סמוכים באי-בי שבחרנו, דיוק זה אמור לתת טווח בטחון מספק בכדי למנוע ׳זליגה׳ בעת קליטת צליל (בחירה שגויה של צליל סמוך).

מתוקף העובדה כי מעטים הם המקרים בהם מיקרופון קולט צליל יחיד ונקי ללא רעשים (בכל זאת, אנחנו חיים בעולם רועש...), ישנן טכניקות בהן ניתן להשתמש ע״מ להפחית את רעשים אלה ולהגדיל את הדיוק.

לדוגמא, ניתן להשתמש בפילטר המתמטי- Low-pass filter [16] בכדי לנפות צלילי קיצון טרם שלב פענוח התדרים באמצעות פונקציית FFT (Fast Fourier Transform), פעולה שאמורה לשפר את הדיוק בקליטת הצלילים ובכך להקטין את זמן השליחה הנדרש של כל צליל.

מכיוון שמימוש של פילטר כזה הוא מסובך יחסית, במקומו הוכנס קוד אשר מממש את היוריסטיקה הבאה (אשר מזכירה מאד את הפילטר לעיל)- התעלמות מכל תדר נמוך מ-300 הרץ או גבוה מ-2000 הרץ. קוד זה מסייע לנו להתעלם מהפרעות באמצעות התעלמות מצלילים נקלטים בעלי תדר מחוץ לטווח אותו אנחנו מצפים לקלוט.

מתוך ניסיונות הרצה רבות, ניכר כי זמן השידור האופטימלי של כל צליל, ע״מ שייקלט ברמה סבירה ע״י הצד המקבל, הוא מחצית השניה.

האלגוריתם בו אנו עושים שימוש לצורך קליטת רצף הצללים המרכיבים את המסר-

א. כאשר מופיע צליל התחלת עסקה מהקונה מתחילים את תהליך קליטת המסר.

ב. מתייחסים לקליטת צליל התחלת העסקה כנקודת ייחוס, ומתחילים לספור את השניות שעוברות מאותה נקודה. בכל חלון של חצי שניה אנו מצפים לקלוט תדר יחיד.

ג. בכל חלון של חצי שניה, אנו קולטים מספר מסוים של דגימות, תלוי במספר פרמטרים.

ד. כל דגימה היא למעשה מערך של כלל התדרים (בעיגול מסוים אשר תלוי במספר פרמטרים כגון גודל החוצץ), אשר עבור כל תדר מופיע ערך הדיצבל (עוצמת התדר המשודר) אשר נקלט עבור אותו התדר. המערך מתקבל באמצעות ביצוע פונק׳ FFT על גבי הקלט הגולמי הנקלט ע״ג החוצץ.

ה. עבור כל דגימה אנו מתייחסים לתדר אשר נשמע בדציבלים הגבוהים ביותר באותה הדגימה כתדר המייצג את אותה הדגימה.

ו. במידה והתדר המייצג חורג מגבולות הפילטר (נמוך מ-300 הרץ או גבוה מ-2000 הרץ), נבדוק את התדר השני בעוצמתו. אם גם השני חורג מגבולות הפילטר, נשליך את דגימה זו.

ז. אנו מונים בכל חלון של חצי שניה את כמות מופעי מייצגי דגימות שונים ע״י שימוש באובייקט של המחלקה FrequenciesCounter.

ח. תדר מוגדר כתדר השולט באותו חלון של חצי שניה, אם 60% ומעלה מכלל הדגימות באותו חלון היו של אותו תדר מייצג. במידה באותו חלון אף תדר לא עבר את סף ה-60% אנו נאלצים להפסיק את תהליך קליטת המסר וחוזרים להמתין לצליל התחלת העסקה. במידה והצלחנו למצוא כזה תדר, אנו מכניסים את אותו הצליל לרשימת התדרים הנבנית, ועוברים לקלות את התדר של החלון הבא.

ט. קליטת המסר מסתיימת כאשר נקלט צליל סיום עסקה. באותה נקודה אנו גם מפסיקים את תהליך קליטת הצלילים ומעבירים את המסר הנקלט לשלבי אימות המסר.

5.7. אימות המסר הנקלט

כאמור, אנו מזהים כי קיים מסר בתהליך שליחה ומתחילים לקלוט אותו כאשר נקלט צליל התחלת עסקה, אנו יודעים כי שידור המסר הסתיים כאשר מתקבל צליל סיום עסקה. כעת, כאשר המסר בידינו אנו מעוניינים לוודא כי הוא התקבל כהלכה. הבדיקות אשר מתבצעות הן-

- צליל בדיקת סיכום ביקורת- אנו מבצעים על המסר הגולמי את פונק׳ סיכום הביקורת ומשווים את המסר שהתקבל עם סיכום הביקורת כפי שחושב בצד השולח.
- צליל שלב- אנו מוודאים כי צליל השלב ($S_1/S_2/S_3$) של המסר שהתקבל תואם לשלב בו אנו נמצאים כעת.
- גודל המסר- מוודאים כי גודל המסר המתקבל תואם את הגודל אותו אנו מצפים לקבל, אשר מורכב מסכום גדלי השדות הרלוונטים לאותו שלב.

5.8. שידור צלילים

שידור הצלילים יתבצע ע״י שימוש ברמקול המכשיר החכם. בכדי לעלות את הסיכוי להצלחת העסקה, בעת כניסה ליישומון, עוצמת הקול המשודר לרמקול יוגדר באופן אוטומטי למקסימום. בעת היציאה מהיישומון, עוצמת הקול המוגדרת תחזור באופן אוטומטי לערך המקורי.

6. הנחות המערכת

כמובן שברצוננו לדמות ככל האפשר מערכת מסחרית המממשת ארנק דיגיטלי מבוסס תמסורת קול. מתוקף מגבלות שונות, נאלצתי לבצע מספר הנחות מקלות-

- מכיוון שאין ביכולתנו לבצע עסקה הכוללת העברת כספים הלכה למעשה, המערכת מבצעת סימולציה בלבד של ביצוע עסקה אל מול הבנק. ה״עסקה״ מתבצעת ע״י שרת הקצה באמצעות קריאה לפונקציה 'performTransaction', אשר למעשה איננה מבצעת דבר (פונק׳ ריקה אשר תמיד מחזירה ערך חיובי). במידה ונרצה להפוך את המערכת לכזו שיודעת לבצע עסקאות אמת, כל שנצטרך לעשות הוא לממש את הפונקציה הזו.
- לצורך ההדגמה, הערך המספרי של הסכום לתשלום בעסקה הינו מספר רנדומלי המוגרל טרם תחילת העסקה.
- כלל בקשות ההתקשרות המתבצעות אל מול שרת הקצה מתבצעות בפרוטוקול HTTP ללא הצפנה, מסיבה זו שרת הקצה מאזין אך ורק בפרוטוקול זה. באופן פשוט למדי, ניתן יהיה להחליף את השימוש בפרוטוקול HTTP ל-HTTPS. לשם כך על שרת הקצה יהיה לייצר מפתח פרטי וסרטיפיקט.
- בעבודה המסכמת תיארנו כי בתהליך הרשמת הקונה, מכשיר הקונה מנפיק באופן חד פעמי מפתח פרטי ופומבי (לצורך הפתרון מבוסס ההצפנה), ושולח את המפתח הפומבי לשרת הקצה בעזרת מעטפת של CSR (Certificate signing request). שרת הקצה יחתום על המפתח הפומבי ובכך יהפוך אותו לסרטיפיקט. בפרויקט זה, בכדי להימנע ממימוש CA (Certificate Authority), לאחר שמכשיר הקונה ינפיק את זוג המפתחות, הוא ישלח את המפתח הפומבי ללא המעטפת ה-CSR. כמו כן, שרת הקצה לא יחתום על המפתח הפומבי וישתמש בו (ישלח אותו למכשירי המוכרים) באופן גולמי.
- ההצפנה ותהליך יצירת המפתחות יתבצע בפרוטוקול RSA. המפתחות ישמרו בפורמט Base64.
- חישוב סיכום ביקורת- הפונק׳ שבחרנו להשתמש עבור בדיקת סיכום הביקורת היא ממוצע פשוט של תדרי המסר, אך כמובן שישנן אפשרויות רבות אחרות (כגון שימוש בפונקציית מודולו וכו׳).
- בעת כל התקשרות של מכשיר המוכר לעבר שרת הקצה, מכשיר המוכר ישלח לעבר השרת בין היתר את שם המשתמש והסיסמא שלו ובכך למעשה יבצע פעולת Login בכל פעם מחדש. ברור כי במימוש מסחרי, הגיוני יהיה לממש תהליך Login ייעודי שלאחריו ישמר Session פתוח, כך יחסך תהליך ביצוע ה-Login בכל בקשה מחדש (דבר שבמידה מסוימת גורע מביצועי המערכת).
- הצטרפות מוקדמת לשירות- ההנחה היא שהקונים והמוכרים קיבלו את שם המשתמש והסיסמא האישי בתהליך ראשוני כלשהו (באמצעות הטלפון, האי-מייל וכו׳).
- לא תינתן אפשרות להוסיף משתמשים חדשים לשרת הקצה. בזמן התקנת היישומון, טבלאות המשתמשים בשרת הקצה ימולאו בנתוני משתמשים קבועים, כאשר לטבלה Buyers יוכנסו 10 שמות קונים- buyer1-buyer10, ולטבלה Sellers יוכנסו 10 שמות קונים- Sellers1-Sellers10

- אנו נתייחס לשרת הקצה כישות אחידה, זאת למרות שבמימוש מסחרי סביר להניח כי יהיו מעורבים שרתים נפרדים עבור כל תפקוד פונקציונלי (שרת מולו מכשיר המוכר מבצע את העסקה, שרת הדואג לביצוע הטרנזקציה הכספית, שרת מסד נתונים וכו').

7. עיצוב מערכת תוכנה

7.1. תיאור רכיבים עיקריים

בטבלה הבאה נתאר את המחלקות בהם אנו עושים שימוש-

	שם המחלקה	תיאור
Activities	MainActivity	מנהלת את הActivity הראשי של התוכנית ממנו ניתן לנווט לActivity של הקונה ולזה של המוכר. כמו כן ניתן לבחור את האלגוריתם ולהרים את השרת
	BuyerActivity	מנהלת את הActivity של מכשיר הקונה
	SellerActivity	מנהלת את הActivity של מכשיר המוכר
	BuyerConfigurationActivity	מנהלת את הActivity שבעזרתו הקונה רושם לראשונה את חשבונו
	SellerLogin	מנהלת את הActivity של ביצוע Login של המוכר
Activities sub-classes	BuyerStateMachine	אובייקט 'Single-tone' המנהל את מכונת המצבים של פעולות הקונה
	SellerStateMachine	אובייקט 'Single-tone' המנהל את מכונת המצבים של פעולות המוכר
Fragments	RecordFragment	מנהלת את הFregment אשר מטפל בתהליך קליטת הקול ומציג את התהליך בשני ה-Activities של המוכר ושל הקונה
	SoundTransmissionFragment	מנהלת את הFregment אשר מציג את תהליך שידור הקול בשני ה-Activities של המוכר ושל הקונה
מחלקות	SoundRawTransmission	מחלקה אשר אחראית על תהליך קליטת הקול

	SoundTransmission	יורשת מהמחלקה הקודמת ומלבישה את שכבה המאפשרת להתייחס למסר הקולי כרצף של תווים כמו כן מוסיפה תקורה בדמות סיכום ביקורת, צליל שלב וצלילי התחלה וסיום.
	FieldsSizes	מחלקה המכילה את גדלי השדות המרכיבים את המסרים הקוליים הנשלחים/מתקבלים ומוודאת את תקינות גודלם
	FrequenciesCounter	מחלקה המונה את כלל התדרים אשר נקלטו באותו חלון של חצי שניה זאת ע״מ לאתר את התדר המוביל
	NameValuePair	מימוש עזר הנועד לאחסן זוגות של מפתח מול ערך. נועד בכדי לשלוח מידע לשרת הקצה
	ProtocolParameters	אובייקט Single-tone אשר אחראי לשמור על כלל משתני המערכת
	ReturnedStatus	מחלקת עזר אשר נועדה בכדי להעביר בין אובייקטים סטטוס של הצלחה/כישלון (כולל תיאור הכישלון)
	WebServer [10]	המימוש של שרת הקצה
מחלקות סטטיות	Auxiliaries	מחלקה המכילה מגוון פונקציות שירות
ספריות חיצוניות	FFT [11]	מחלקה שתפקידה חישוב אריתמטי של פונקציית Fast Fourier Transform הנועדה לפענוח הקול הנקלט למרכיבי תדריו
	Libotp [12]	מחלקה שתפקידה חישוב אריתמטי של ה-Token (TOTP)
	Complex [13]	מחלקה המממשת אחסון של מספרים מרוכבים. תפקידה לאחסן את התוצרים של פונק׳ FFT

7.2. כלי פיתוח והפצת היישומון

שפת פיתוח	**Java for android**
סביבת פיתוח IDE	Android Studio version 2.3.3
מערכת ניהול בסיסי נתונים	SQLite DB

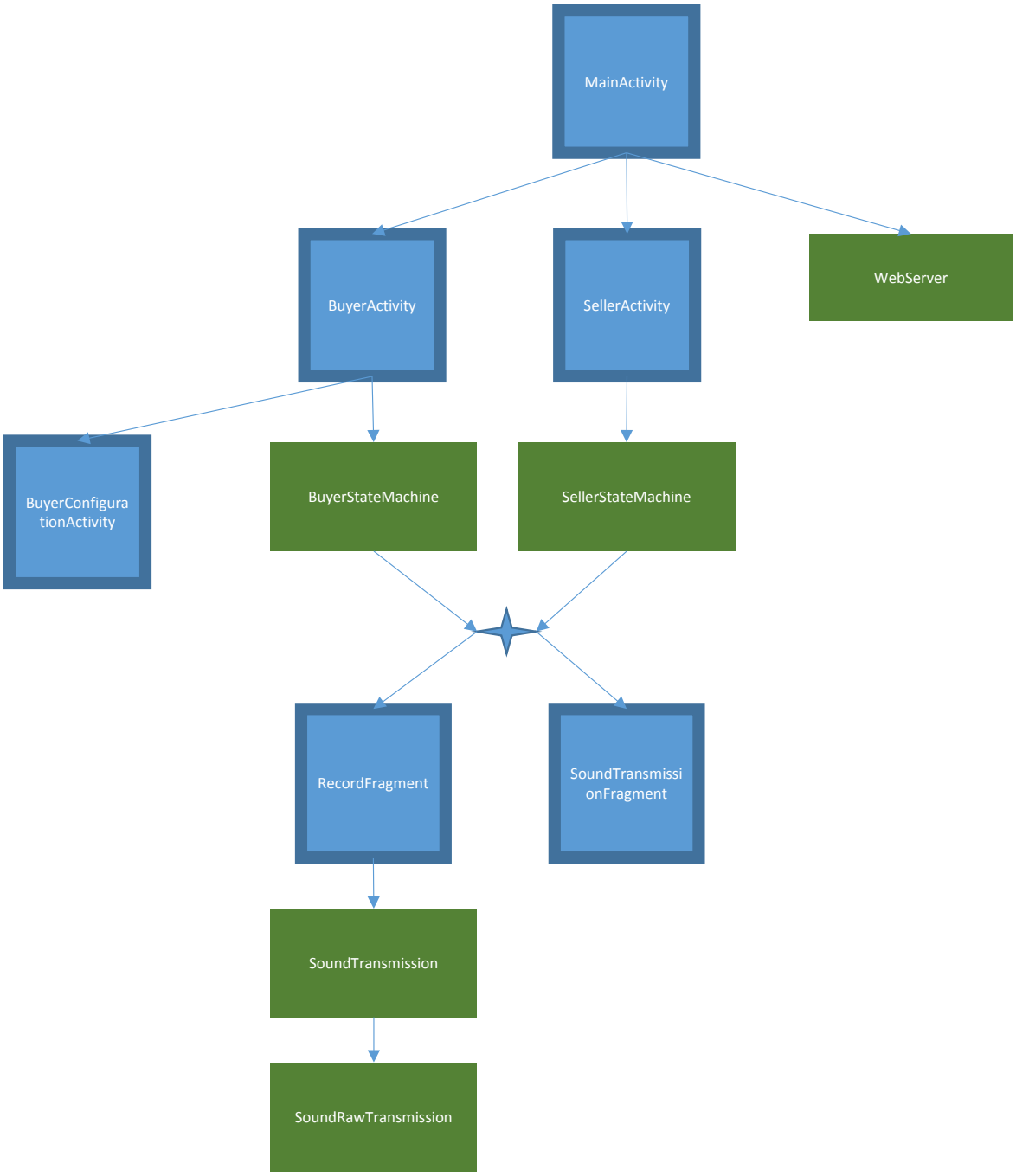
התקנת היישומון על גבי המכשיר החכם ניתנת לביצוע באמצעות מספר חלופות-

- הרצת קוד המקור באמצעות סביבת הפיתוח Android Studio על גבי המחשב האישי וחיבורו למכשיר החכם ע״י שימוש בכבל USB.
- הכנסת קובץ התוצר של קמפול הקוד (קובץ apk) כקובץ למכשיר החכם והתקנתו ע״י הפעלת הקובץ במכשיר. ניתן לשלוח את הקובץ למכשיר ע״י שליחתו באימייל, כבל USB וכ״ו...
- עתידי- העלאת קובץ ה-apk לחנות האפליקציות של Android המכונה- Google Play.

7.3. ארכיטקטורת מחלקות

להלן תרשים (איור 2) המתאר את היחסים שבין מחלקות הפרויקט, כאשר-

- מחלקה בצבע כחול מסמלת את העובדה שהמחלקה מקושרת גם ל-Activity או Fragment. במילים אחרות- המחלקה אחראית על בניית המסך הרלוונטי בכך שהיא מקושרת לקובץ ה-xml המתאים האחראי על אותו המסך.
- מחלקה בצבע ירוק היא מחלקה רגילה שלה מופע יחיד (Single-Tone).
- חץ ממחלקה א׳ למחלקה ב׳ מעיד על כך שמחלקה א׳ היא זו שיצרה את מחלקה ב׳.


MainActivity
BuyerActivity
SellerActivity
WebServer
BuyerConfigura
tionActivity
BuyerStateMachine
SellerStateMachine
RecordFragment
SoundTransmissi
onFragment
SoundTransmission
SoundRawTransmission

-איור 2-

7.4. תיאור תהליך ההתחברות לשרת הקצה

במהלך העסקה (ועבור מכשיר הקונה, גם פעם אחת לפניה) מכשיר המוכר נדרש לבצע פניות חוזרות ונשנות לעבר שרת הקצה. פניות אלו מבוצעות על גבי תשתית HTTP. מבנה פניות אלו, כמו גם המסר החוזר מן שרת הקצה, נבנו בפורמט JSON סטנדרטי.

להלן תיאור כלל ה- URIs (כתובות Http) בהם עושים שימוש מכשירי מוכר והקונה בעת פנייה תקשורתית לשרת הקצה-

א. פניית מכשיר מוכר לשרת הקצה

בכלל הפניות של מכשיר המוכר לשרת הקצה הפניה מתבצעת תוך שליחת המשתמש והסיסמא של המוכר- SellerUser ו-SellerPassword (לצורך הזדהות מול השרת). שרת הקצה יאשר את ההתקשרות ויסכים לשלוח מידע בערוץ החזור אך ורק במידה והוא הצליח לבצע אימות מוצלח.

- seller/get-buyer-certificate

רלוונטי בלבד לעסקה אשר נעשה בה שימוש בפרוטוקול ההצפנה.

כפי שתיארנו בטבלת מהלך מעבר הנתונים בפרוטוקול אשר תוארה בפרק אשר תאר את פרוטוקול ההצפנה, מכשיר המוכר ישלח לעבר שרת הקצה את מזהה הקונה- BuyerId. במידה ושרת הקצה מכיר את מזהה הקונה, בערוץ החוזר של ההתקשרות שרת הקצה ישדר למכשיר המוכר את $Ctr_{BuyerPubKey}$ שהוא למעשה המפתח הפומבי של הקונה. לצורך הגברת האבטחה ניתן לשדר במקום המפתח סרטיפיקט אשר יכיל בתוכו את המפתח (ישנה התייחסות לכך בפרק הנחות המערכת).

- seller/get-token2

רלוונטי בלבד לעסקה אשר נעשה בה שימוש בפרוטוקול TOTP.

כפי שתיארנו בטבלת מהלך מעבר הנתונים בפרוטוקול אשר תוארה בפרק אשר תאר את פרוטוקול TOTP, מכשיר המוכר ישלח לעבר שרת הקצה את מזהה הקונה- BuyerId ואת שאר נתוני העסקה- TransPrice, BusinName, MaxPmt, Token1, במידה ושרת הקצה מכיר את מזהה הקונה ומאמת בהצלחה את Token1, בערוץ החוזר של ההתקשרות שרת הקצה יחשב וישדר למכשיר המוכר את Token2 הרלוונטי לאותו זמן המורכב בין השאר מהנתונים שנשלחו לשרת ומ-HwId הסודי של מכשיר הקונה אשר עליו שרת הקצה מכיר ושומר.

- seller/get-server-confirmation

רלוונטי לשני סוגי הפרוטוקולים.

כפי שתיארנו בטבלת מהלך מעבר הנתונים בשני הפרוטוקולים, מכשיר המוכר ישלח לעבר שרת הקצה את מזהה הקונה- BuyerId ואת נתוני העסקה- TransPrice, ChosenPmt. בפרוטוקול TOTP ישלח גם כן Token3. במידה ושרת הקצה מכיר את מזהה הקונה, אימת שהעסקה יכולה להתבצע (לדוגמא, אימת כי מסגרת האשראי של הקונה מספיקה ע״מ לבצע את סכום העסקה), ואימת את Token3 (אם רלוונטי), השרת יחזיר בערוץ החזור הודעה על הצלחת/כישלון העסקה.

- seller/test-connection

רלוונטי לשני סוגי הפרוטוקולים.
משמש לבדיקה ראשונית של התקשורת ממכשיר המוכר לשרת הקצה בעת הזנת פרטי המשתמש והסיסמא. בנוסף לאישור פרטי המשתמש, שרת הקצה מחזיר גם את שם בית העסק לצרכי תצוגה במסך המוכר ביישומון.

ב. מהלך הרשמה ראשונית - פניית מכשיר קונה לשרת הקצה

- Buyer/registration

בכדי שקונה יוכל להתחיל להשתמש בשירות הארנק הדיגיטלי, תחילה עליו לבצע תהליך הרשמה ראשונית אל מול שרת הקצה. חשוב להדגיש כי תהליך זה צריך להתבצע אך ורק פעם אחת ותקף למספר רב של עסקאות, ובכך נשמרת ההנחה כי אין צורך בחיבור אינטרנטי בין מכשיר הקונה לשרת הקצה בזמן ביצוע העסקה.
פניה זו מתבצעת תוך שליחת המשתמש והסיסמא של הקונה- BuyerUser ו-BuyerPassword (לצורך הזדהות מול השרת). כפי שציינו, את נתוני ההזדהות הקונה קיבל עוד מראש בעת ההצטרפות לשירות התשלומים. שרת הקצה יאשר את ההתקשרות ויסכים לשלוח מידע בערוץ החזור אך ורק במידה והוא הצליח לבצע אימות מוצלח. כמו כן, מכשיר הקונה ישלח לעבר שרת הקצה את מזהה המכשיר- DeviceId ואת המפתח הפומבי $Ctr_{BuyerPubKey}$ (אשר ישמש לצורך עסקאות בהן יעשה שימוש בפתרון ההצפנה שהצגנו). שרת הקצה ינפיק באותה פניה, יאכסן ויחזיר למכשיר הקונה בערוץ החזור את מזהה הקונה- BuyerId ואת שלושת המזהים הסריאלים serial1-3 (בהם ישתמש לצורך עסקאות בהן יעשה שימוש בפתרון TOTP שהצגנו).

7.5. תיאור פונקציות עיקריות

נתאר בטבלה להלן את פונקציות השירות העיקריות שפיתחנו במהלך הפרויקט-

פונק'	תיאור
getCurrentTime	מחזירה את הזמן הנוכחי בשניות
postAndGetJsonDataFromUrl	שולחת רשימת של ערכים לשרת היעד בפורמט JSON ומחזירה את התגובה גם היא בפורמט JSON
listToJson	ממירה מטיפוס של רשימה לטיפוס JSON לצורך שליחה ברשת
generateRandomPrice	מייצרת מחיר רנדומלי (בין 1 ל 100)
Encrypt	מצפינה מסר באמצעות מפתח פומבי אסימטרי
Decrypt	מפענחת מסר באמצעות מפתח פרטי אסימטרי
stringToPublicKey	ממירה מפתח פומבי השמור בפורמט Base64 לפורמט מפתח פומבי סטנדרטי
stringToPrivateKey	ממירה מפתח פרטי השמור בפורמט Base64 לפורמט מפתח פרטי סטנדרטי
publicKeyToString	ממירה מפתח פומבי למחרוזת בפורמט Base64
privateKeyToString	ממירה מפתח פרטי למחרוזת בפורמט Base64
getDeviceId	מחזירה מחרוזת אשר מאפיינת באופן חח"ע את מכשיר הקונה (טלפון חכם)
generateToken	מייצרת TOKEN בגודל נתון (מסר מספרי תוצר של פונק' גיבוב) המורכב ממחרוזת ומהדקה הנוכחית
generateTokenForSpecificTime	מייצרת TOKEN בגודל נתון (מסר מספרי תוצר של פונק' גיבוב) המורכב ממחרוזת ומדקה נתונה. משתמשים בה בכדי לייצר TOKENים השייכים לדקות סמוכות, זאת בכדי לנטרל גורם של אי סנכרון מדויק בין השעונים
verifyToken	מוודאת כי Token נתון ע"י יצירת Token בעצמה וביצוע השוואה ביניהם
createKeyPair	מייצרת מפתח אסימטרי המיוצג באמצעות טיפוס מסוג KeyPair
getPrivateKey	מחלצת מהטיפוס KeyPair את המפתח הפרטי

getPublicKey	מחלצת מהטיפוס KeyPair את המפתח הפומבי
generateIdentifier	מייצר מחרוזת בגודל נתון המורכב מרצף רנדומלי של ספרות ואותיות
charToFrequency	ממירה תו נתון בפורמט Base64 לערך תדר הקול של אותו התו (ע״פ מיפוי קבוע)
frequencyToChar	ממירה ערך תדר קול נתון לתו בפורמט Base64 (ע״פ מיפוי קבוע)
adjustFrequencyToMultiple	מקבל ערך תדר קול ומעגלת את ערכו ע״פ שיעור נתון
getChecksumOfFrequencyArray	מקבלת מערך של תדרי צלילים ומחשבת את סיכום הביקורת
intToStringWith0Padding	מקבלת מחרוזת המכילה ספרות ומוסיפה לה '0 ע״פ ערך מקסימום נתון
addSpacesPaddingToString	מקבלת מחרוזת ומוסיפה לה רווחים ע״פ ערך מקסימום נתון

7.6. שירותי גישה למסד נתונים

מתוך הצורך של שרת הקצה לשמור נתונים במסד נתונים קשיח (שאינו נמחק לאחר היציאה מהיישומון), אנו נשתמש בפרקטיקה נפוצה למימוש מסד נתונים תחת סביבת Android באמצעות תכונה מובנית של מע״ה הנקראת-SQLite DB. זהו למעשה DB פשוט לשימוש אשר מובנה במע״ה Android ואשר ניתן לבצע מולו שאילתות SQL סטנדרטיות.

ע״מ להשתמש ב- SQLite אנו נייבא את המחלקות הבאות:

android.database.sqlite.SQLiteOpenHelper

android.database.sqlite.SQLiteDatabase

טבלאות שרת הקצה:

שם טבלה	עמודה 1	עמודה 2	עמודה 3	עמודה 4	עמודה 5	עמודה 6	עמודה 7	עמודה 8
Buyers	**User**	**Password**	**buyerId**	**serial1**	**serial2**	**serial3**	**buyerPublicKey**	**deviceId**
Sellers	User	Password	sellerId	businessName				

בזמן התקנת היישומון, שתי הטבלאות ימולאו בנתוני משתמשים קבועים-

לטבלה Buyers יוכנסו 10 שמות קונים- buyer1-buyer10, ולטבלה Sellers יוכנסו 10 שמות קונים- Sellers1- Sellers10. נקבע סיסמא זהה לשם המשתמש.

8. ממשק המשתמש

נתאר את חוויית המשתמש מנקודת הראות של הקונה והמוכר אל מול מכשירי המוכר והקונה, זאת מבלי להיכנס לתיאור השדרים העוברים בין הרכיבים עצמם.

תיאור זה הוא כללי ורלוונטי עבור שני הפרוטוקולים הנתמכים (Encryption/TOTP).

נחלק את התיאור לשני חלקים-

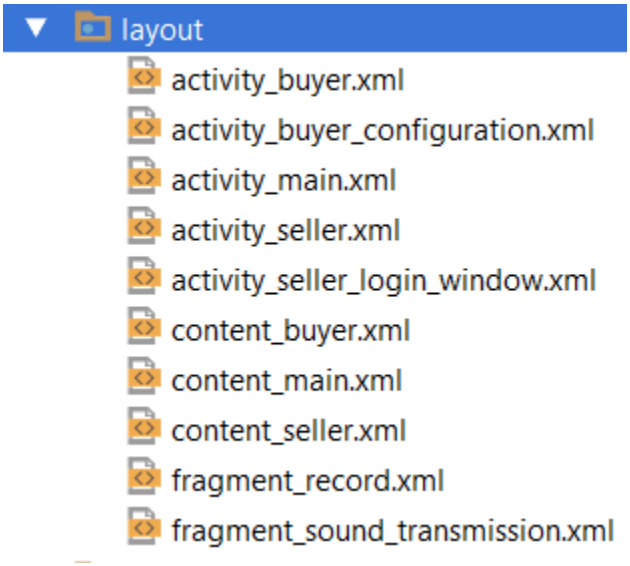
1. אלו מהמסכים הרלוונטים טרם העסקה (תהליך ההרשמה לשירות של הקונה, ביצוע הזדהות מוכר מול שרת, כניסה ליישומון)
2. מסכים בהם נעשה שימוש במהלך העסקה עצמה

נשתמש בסימונים הבאים-

 - עבור מסך במכשיר המוכר

 - עבור מסך במכשיר הקונה

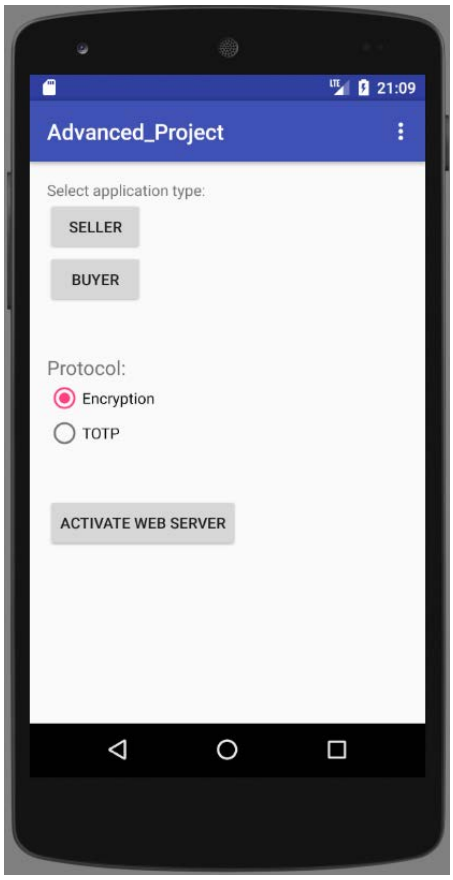
להלן (איור 3) שמות המסכים ביישומון המיוצגים ע"י רשימת קבצי XML בהם מוגדר עיצוב המסכים-



-איור 3-

8.1. מסכים/חוויית משתמש טרם העסקה:

צג קונה ומוכר- כניסה ליישומון. זהו ה-Activity הראשי של התוכנית. מסך זה מוצג בכל פעם אשר נכנסים ליישומון (Activity_main)-



-איור 4-

מסך זה (איור 4) הינו המסך הראשי והראשון אותו רואה המשתמש כאשר הוא נכנס לאפליקציה. שיטת העבודה שבחרנו היא אפליקציה אחת אשר תשרת את כל הרכיבים המעורבים. על המוכר ללחוץ על כפתור הSeller בכדי לעבור לSellerActivity. על הקונה ללחוץ על כפתור הBuyer בכדי לעבור לBuyerActivity. בשני המקרים, לפני הכניסה לmode קונה/מוכר יש לבחור גם כן את הפרוטוקול המתאים- Encryption/TOTP.

בתחתית המסך ממוקם כפתור "Activate Web Server", תפקידו הוא להפעיל ולהריץ כ-Thread ברקע את צד שרת הקצה. מרגע הלחיצה, המכשיר הסלולארי יחל להאזין לתמסורת Http בפורט 8080. מובן כי
ישנן 2 צורות עבודה-

כאשר נכנסים ליישומון מופיע מסך כללי הבורר בין מצבים שונים בהם היישומון מסוגל לפעול-

א. לחצן מעבר למסך קונה- כאשר המשתמש הוא קונה.

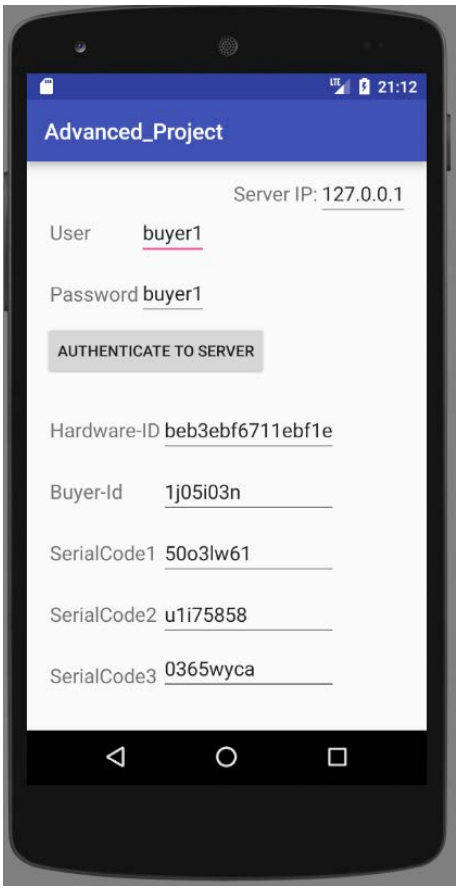
ב. לחצן מעבר למסך מוכר- כאשר המשתמש הוא מוכר.

ג. בחירה בין שני הפרוטוקולים (TOTP/Encryption)- הבחירה מגדירה את הפרוטוקול המופעל הן במידה ונלחץ לאחר מכן על כפתור המעבר למסך הקונה והן למסך המוכר.

ד. לחצן הפעלת/כיבוי תהליכון שרת קצה- לחצן המפעיל תהליכון המדמה את שרת הקצה. התהליכון מרים לאוויר Http-Web-server המאזין בפורט 8080.

בשימוש אמיתי שרת זה כמובן לא ירוץ על גבי יישומון, ע״כ פיתוח זה נעשה ע״מ להקל את תהליך ההדגמה. השרת יכול לרוץ במקביל לריצת היישומון בצורת עבודה של מכשיר קונה או בצורת עבודה של מכשיר מוכר. אפשרי כמובן גם להריץ את השרת לבדו ללא הרצה של תכונה נוספת במקביל, זאת ע״י השארות במסך הכניסה לאפליקציה.

1. **צג קונה**- מסך הרשמת קונה (Activity_buyer_configuration):



-איור 5-

מסך זה (איור 5) מופעל פעם אחת, כאשר הקונה מעוניין להירשם לשירות התשלומים.

- על המשתמש להזין-

- משתמש וסיסמא- נתונים אלו משמשים אותו בכדי להזדהות אל מול שרת הקצה של השירות.
    - ההנחה היא כי הקונה נרשם מבעוד מועד לשירות (באמצעות הטלפון/דרך אתר אינטרנט וכ״ו), ובמעמד זה הונפקו עבורו נתוני המשתמש והסיסמא.
- כתובת ה-IP של שרת הקצה- שדה זה נועד אך ורק בכדי להקל על הדגמת היישומון. ביישומון מסחרי סביר להניח כי השם הDNS-י של שרת הקצה היה נכתב באופן סטטי בקוד היישומון.

o במסך כמו כן מוצגים-

- Hardware-id- מחרוזת אשר נועדה לזהות את מכשיר הקונה באופן חח״ע. בכל מכשיר טלפון חכם/טאבלט נצרבת ע״ג חומרת המכשיר ע״י היצרן מחרוזת המזהה באופן חח״ע את המכשיר. המחרוזת מתקבלת באמצעות שימוש בפונק׳ getDeviceId אשר תוארה מקודם. אנו משתמשים גם בנתון זה בכדי להרכיב את ה-token כאשר הקונה והמוכר משתמשים בפרוטוקול המבוסס על TOTP.
- Buyer-id- מחרוזת אשר מונפקת ע״י שרת הקצה ונועדה לזהות את הקונה באופן חח״ע. ה-token-ים אשר מונפקים בעת שימוש בפרוטוקול TOTP מורכבים גם מנתון זה.
- Serial-code1-3- 3 מחרוזות אשר מונפקות עבור הקונה ומשמשות בכדי לייצר את שלושת ה-token-ים.

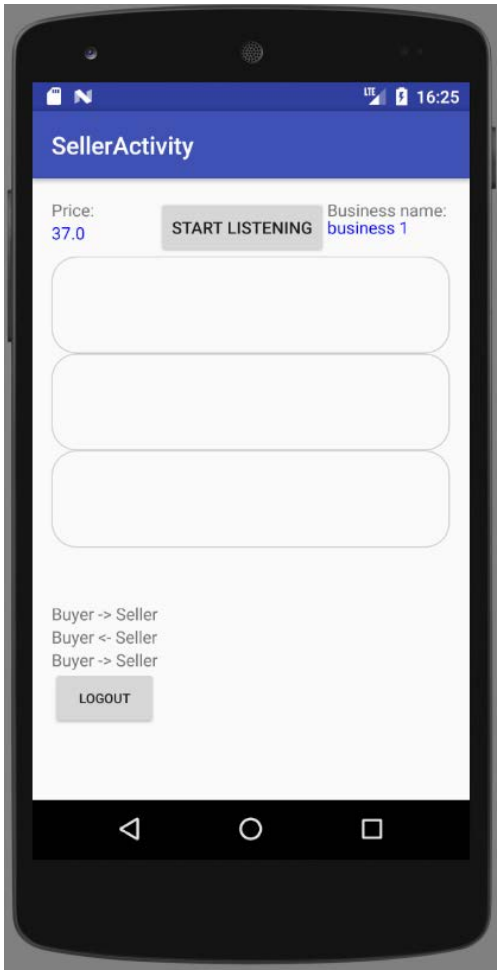
2.  **צג מוכר**- התחברות/הזדהות אל מול שרת הקצה (Activity_seller_login_window):

-איור 6-

בעת הכניסה למסך (איור 6) על המוכר לבצע פעולת התחברות (login) חד פעמית אל מול שרת הקצה. במעמד זה על המוכר להזין את המשתמש ואת הסיסמא אשר הונפקה לו במעוד מועד (לדוגמא, כאשר המוכר מפעיל את היישומון בתחילת היום).

8.2. מסכים/חוויית משתמש במהלך עסקה כללית:

1.  **צג מוכר**- הצגת מחיר עסקה ושם בית העסק (Activity_seller)

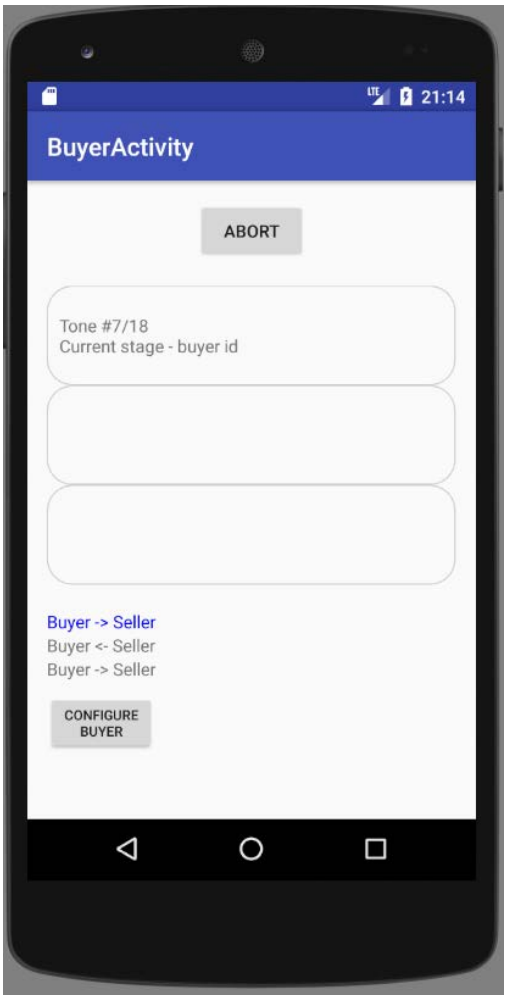


-איור 7-

ניתן להקביל זאת לקופה רושמת של בית העסק אשר מציגה את מחיר העסקה לפני שהלקוח מוציא את ארנקו ע״מ לשלם (איור 7).

במימוש זה, בכדי להתחיל להאזין לתמסורת מהלקוח, על המוכר ללחוץ על לחצן 'START LISTENING'.

2. **צג קונה**- הפעלת עסקה (Activity_buyer)



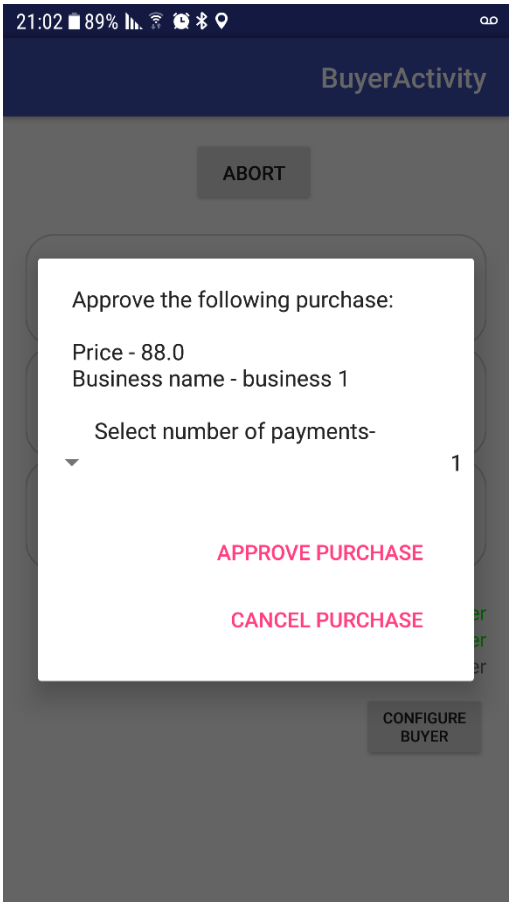
-איור 8-

הקונה הוא היוזם של התחלת ביצוע תהליך התשלום באמצעות ארנק דיגיטלי מבוסס קול. ככזה, מכשירו הוא הגורם הראשון המשדר מסר קולי בתחילת העסקה. מכשיר המוכר באופן תמידי נמצא בהאזנה בכדי לקלוט את מסר התחלת העסקה המתואר.
בכדי להתחיל בעסקה על הקונה ללחוץ על כפתור התחלת עסקה (ראה איור 8).

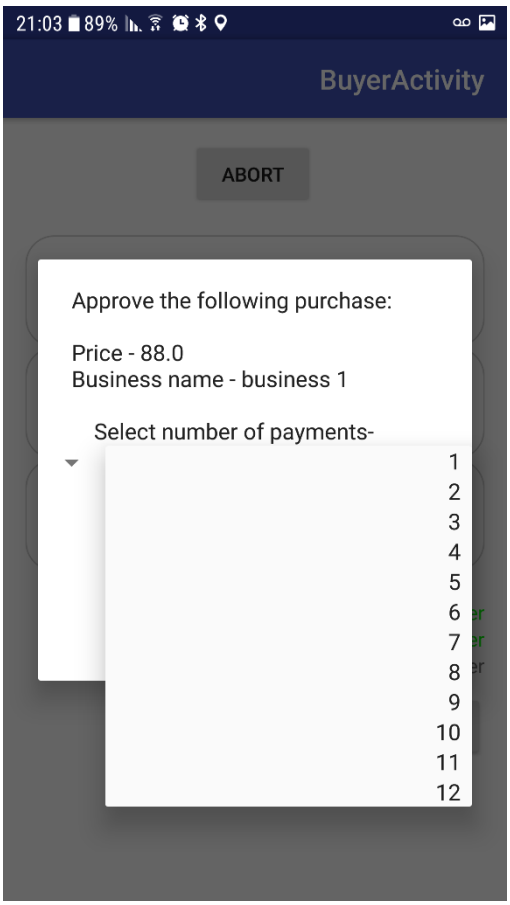
3. **צג קונה**- אישור קונה

לאחר העברת מסרים קוליים בין מכשיר הקונה ומכשיר המוכר, והתקשרות רשתית בין מכשיר המוכר לשרת הקצה, הקונה נדרש לאשר את העסקה במכשירו (איור 9).

מכשיר הקונה מציג את שם בית העסק ומחיר העסקה (נתונים אשר עברו ממכשיר המוכר באמצעות מסרים קוליים). כמו כן, על הקונה לבחור את מספר התשלומים בו הוא מעוניין מתוך רשימה (איור 10). כעת, לאחר שהקונה וידא כי שם בית העסק ומחיר העסקה תואמים את הנתונים המוצגים לו בצג המוכר, על הקונה לתת אישור סופי לביצוע העסקה באמצעות לחיצה על לחצן האישור במכשיר הקונה.



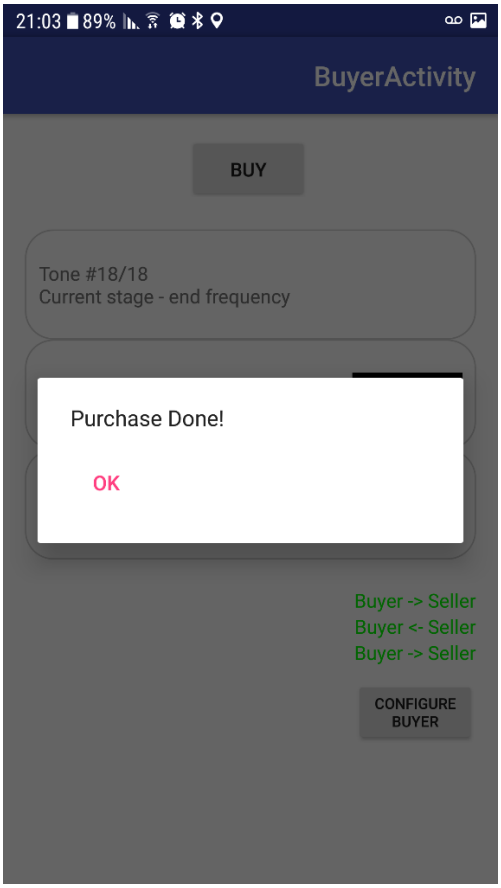
-איור 9-



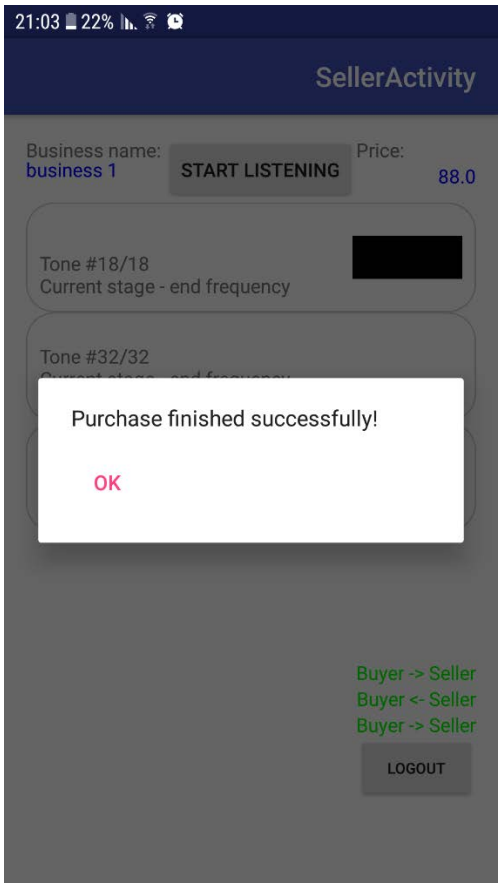
-איור 10-

4.  **צג קונה ומוכר**- חיווי על הצלחת העסקה

לאחר ביצוע העסקה בפועל אל מול שרת הקצה, מכשירי הקונה (איור 11) והמוכר (איור 12) יציג סימולטנית אישור חזותי על הצלחת ביצוע העסקה כך ששני הצדדים ידעו שתהליך התשלום הסתיים.



-איור 11-

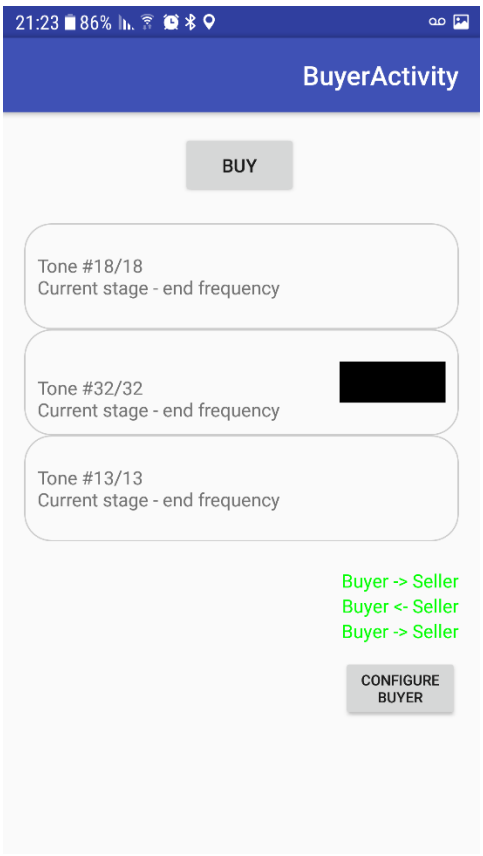


-איור 12-

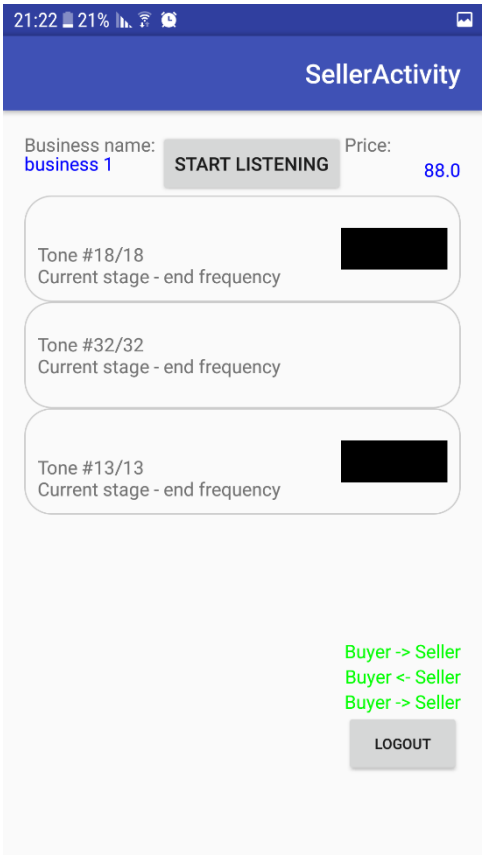
8.3. שימוש ב-Fragments:

נזכיר כי Fragment הוא רכיב תצוגה אשר מאפשר להשתמש בו שימוש רב פעמי, במסכים (Activity) שונים ואף מספר פעמים באותו המסך. אנו בפרויקט עושים שימוש סה"כ בשני Fragments-

- Fragment_record- מופיע במסך הקונה (איור 13) פעם אחת (S_2) ובמסך המוכר (איור 14) פעמיים (S_1, S_3).
- Fragment_sound_transmission- מופיע במסך המוכר (איור 14) פעם אחת (S_2) ובמסך הקונה (איור 13) פעמיים (S_1, S_3).



-איור 13-



-איור 14-

תפקידם של שני ה-Fragments הוא-

- להציג את שם השדה בזמן קבלתו/שליחתו לצד השני.
- להציג בזמן קבלת/שליחת המסר את כמות הצלילים הכללית באותו השלב, ואת מספרו של הצליל המדויק אשר נשלח/מתקבל באותו פרק זמן ספציפי.

בו בזמן שבו Fragment_sound_transmission מציג את תהליך שליחת הצליל של אותו השלב, במכשיר השני Fragment_record יציג את תהליך קבלת הצליל של השלב. המטרה היא שכאשר נתבונן בכל אחד מהמסכים, אנו נראה תצוגה דומה (אמור להופיע אותו הטקסט).

נשים לב כי שלב S_2 של פרוטוקול ההצפנה הוא מקרה מיוחד מכיוון שההנחה היא כי אנו לא יודעים מבעוד מועד בצד המקבל מה יהיה גודלו של המסר המוצפן. לכן כחלק מהפרוטוקול, טרם שליחת המסר המוצפן, אנו שולחים את גודלו.

9. השוואה בין הפרוטוקולים

בעבודה המסכמת הראנו כי שני הפרוטוקולים, אף ששניהם מתבססים על שני אמצעים מתמטיים שונים (הצפנה ושימוש בToken מבוסס זמן), מעניקים פתרון אבטחתי מספק ביותר עבור מתקפות מבוססות 'אדם באמצע'.

מעבר לערך האבטחתי, חשוב יהיה לבדוק האם ישנו הבדל משמעותי בין האלגוריתמים בהיבט חוויית המשתמש. בהתייחסות למשתמש הכוונה היא הן לקונה והן למוכר. נראה שזמן השידור של המסר הקולי הוא המדד המרכזי המאפיין את חוויית המשתמש. ברור כי זמן שידור ארוך מדי (של מסר קולי ארוך) יגרום לפרוטוקול להפוך ללא רלוונטי לשימוש ריאלי. אחת מההנחות הראשוניות אשר התייחסנו אליה בעבודה המסכמת הייתה שהארנק הדיגיטלי אמור למעשה 'להקל על החיים' ע"י כך שהוא יכול לחסוך נשיאה של כרטיס אשראי או כסף מזומן. תשלום באמצעות כרטיס אשראי או כסף מזומן לוקח לכל היותר מספר שניות. אך הגיוני כי התפיסה מאחורי פיתוח פרוטוקול ארנק דיגיטלי מכל סוג שהוא תהיה שלכל היותר לא נרצה להרע את זמן זה.

בעבודה המסכמת, השווינו זמן השידור של שני הפרוטוקולים ע"י סכימה של כמות הצלילים המשודרת בכל פרוטוקול. לאחר ניתוח, קיבלנו כי סך הצלילים אשר ישודרו-

- בפתרון TOTP - 63 צלילים.
- בפתרון ההצפנה עם מפתח של 512 ביט – 122 צלילים.
- בפתרון ההצפנה עם מפתח של 1024 ביט – 206 צלילים.

זמן שליחת המסר

כאמור, מניסיונות שערכתי זמן השידור האופטימלי של כל צליל, ע"מ שייקלט באופן מיטבי בצד השני, הוא מחצית השניה. מה שאומר שסה"כ משך זמן העסקה באמצעות ארנק דיגיטלי מבוסס קול בפתרון TOTP יהיה כחצי דקה, ומשך הזמן בעת שימוש בפתרון ההצפנה יכול להיות פי 2 או אף 3 מזמן זה. בכל מקרה, סדר הגודל של משך זמנים אלו כמובן איננו מקובל כלל וכלל, מהסיבה שהוא חורג משמעותית מהזמן שלוקח לבצע עסקה באמצעות כרטיס אשראי או מזומן (מספר שניות).

אך לחלוטין אין בעובדה זו בכדי להכחיד את הרעיון החדשני של ארנק דיגיטלי מבוסס קול כאשר בו אין למכשיר הקונה חיבור לשרת הקצה בזמן ביצוע העסקה. זאת למרות כי ברור שהנחת חיבור אינטרנטי של מכשיר הקונה לשרת הקצה (כמו שקיים בכל מימוש אפשרי של ארנק דיגיטלי מבוסס קול כפי שהצגנו בעבודה המסכמת) הייתה מצמצמת מאד את זמן השליחה מכיוון, שמטבעה, דורשת שליחת הרבה פחות מידע באמצעות תמסורת הצליל (כפי שהראנו בעבודה המסכמת, במימושים כאלה רוב המידע עובר דרך התשתית האינטרנטית).

מלבד זאת, ברור כי ניתן לבצע שיפורים רבים באלגוריתם קליטת הקול בו אנו משתמשים, כך ששידור כל צליל יערך הרבה פחות מחצי שניה. אך בפרויקט זה קצרה היריעה מלממש את כולם (כאמור, מתוקף ההתמקדות שלנו בעניין האבטחתי ולא הפיסיקה של הקול, אשר מהווה נושא שלם משל עצמו). בין השיפורים הפוטנציאלים ניתן למצוא-

- כפי שציינו מקודם, ניתן להשתמש בפילטר המתמטי- Low-pass filter [16] בכדי לנפות צלילי קיצון טרם שלב פענוח התדרים באמצעות פונקציית FFT (Fast Fourier Transform), פעולה שאמורה לשפר את הדיוק בקליטת הצלילים ובכך להקטין את זמן השליחה הנדרש של כל צליל.
- סיכום ביקורת- ניתן גם להשתמש בשכבת סיכום ביקורת חזקה הרבה יותר אשר מעבר להתרעה על שגיאה במסר הנקלט, מסוגלת אף גם לתקנו.
- כתיבה בשפה נמוכה יותר- מכיוון ששפת התכנות בה נכתבה העבודה, Java for Android, נחשבת לבזבזנית במשאבים ובעלת ביצועים נמוכים יחסית, לשלב בתוך הקוד מתודות בשפה הקרובה יותר לשפת מכונה. מסיבה זו, פרקטיקה ידועה בפיתוח ישומונים הכוללים קליטת קול בזמן אמת, היא לשלב בתוך הקוד הכתוב בשפת Java for Android מתודות אשר בעצמן כתובות בשפת C.

כמו כן, כפי שציינו בעבודה המסכמת, ישנם מימושים מסחריים אשר קצב השליחה המוצהר בהם הוא טוב יותר מקצב השליחה שהצגנו כאן של 8 ביט לשנייה. לדוגמא-

- Chirp [9]- עם 16 ביט לשנייה. אך כפי שציינו, המימוש מגביל את עצמו לשידור וקליטת צלילים מסוג מאד מסוים אשר מדמים ציוצי ציפורים. סביר להניח שללא הגבלה זו ניתן היה להגיע לתוצאות טובות אף יותר.
- Dhwani [17]- עם 800 ביט לשנייה, זהו קצת גבוה יותר לאין שיעור, אך כפי שציינו, זהו מספר תיאורטי מכיוון ש-Microsoft טרם שחררו פתרון מעשי.
- Zoosh [17]- 300 ביט לשנייה, זהו גם כן קצב גבוה ביותר, אך כאן, כפי שכבר ציינו, ניכר כי לא פורסם דבר על הפתרון לאחר סוף 2011 ולכן צריך לקחת את פתרון זה בערבון מוגבל.

המסקנה שאנו למדים מדיון זה היא שניתן בהחלט להיות אופטימי לגבי הקטנת זמני השידור. לא יהיה מוגזם אף להגיד כי בסבירות גבוהה מאד ניתן יהיה לשפר משמעותית את זמני השידור של הפתרונות שניתחנו, בתוכם פתרון ה-TOTP (כיום 31.5 שניות), פתרון ההצפנה עם 512 ביט (כיום 61 שניות) ואף פתרון ההצפנה עם 1024 ביט (כיום 103 שניות), עד לרמה של שניות בודדות אשר תאפשר שימוש מסחרי בפתרונות אלה.

10. סיכום

המטרה המרכזית בפרויקט זה כהמשך הטבעי של העבודה המסכמת, הייתה להדגים את ישימותו של פרוטוקול ארנק דיגיטלי מבוסס קול **כאשר בו אין למכשיר הקונה חיבור לשרת הקצה בזמן ביצוע העסקה**. מצאנו כי מגבלת אי החיבור לשרת הקצה אכן העלתה אתגרים לא פשוטים הן במישור האבטחתי והן במישור הפרקטי (חווית משתמש), והצלחנו להדגים באמצעות יישומון את פעולותיהם של שני הפתרונות משתי הגישות האבטחתיות השונות- הצפנה א-סימטרית ו-TOTP. באופן זה הראנו כי פתרונות אלה הם ישימים למימוש.

כפי שכבר צוין, כיוון שמטרת פרויקט זה הינה הדגמת הרעיון האבטחתי, הבחירה הייתה להתמקד בשיפור תווך הצליל רק עד גבול סביר בו המסרים יוכלו לעבור ולהיקלט בהצלחה בין שני המכשירים. כפי שהוצג, יש הרבה מקום לאופטימיות ביחס לשיפור זמן השידור ולא צריך לראות בו חסם אף לשימוש מסחרי בפתרון זה.

בעבודה המסכמת התמקדנו בלאתר פתרונות ארנק דיגיטלי מסוג זה אשר מסוגלים להעניק רמת הגנה אבטחתית טובה. במסגרת הפרויקט, הצלחנו להראות כי למרות השונות המרכזית של המנגנון המתמטי שבבסיסם, ניכר כי בשימוש נכון, שני סוגי הפתרון אינם רק ישימים למימוש, אלא בהינתן שיפורים מסוימים מסוגלים אפוא לשמור על זמן עסקה קצר.

בצורה זו הראנו כי למרות שכלל המימושים הקיימים לארנק דיגיטלי מבוסס קול מחייבים לאמץ חיבור אינטרנטי רציף, זוהי איננה גזירת גורל כלל וכלל! ניתן בהחלט לייצר מימושים מסחריים של ארנק דיגיטלי אשר בהם מכשיר הקונה כלל אינו מחובר לאינטרנט. כפי שתיארנו בעבודה המסכמת, זהו יתרון לחלוטין לא מבוטל. אי חיוב חיבור לאינטרנט יגרום לארנק לפעול גם בסיטואציות קיצון (רכישה במקומות ללא קליטה, פסטיבלים בהם חיבור האינטרנט נפל מעומס, נסיעות לחו״ל ועוד) ובכך אף יוכל להגדיל את אמינותו. מפליא אם כך, כי אין בנמצא מימושים קיימים לארנק דיגיטלי מבוסס קול מסוג זה.

11. ביבליוגרפיה (*)

[1] ISO 18092 (ECMA-340). Information technology – Telecommunications and information exchange between systems – Near Field Communication – Interface and Protocol (NFCIP-1)

[2] Housley R., Ford W., Polk W. and Solo D. Internet X.509 Public Key Infrastructure Certificate and CRL Profile. from http://www.rfc-editor.org/rfc/rfc2459.txt , January 1999

[3] Time-based One-time Password Algorithm. In Wikipedia. Retrieved Nov. 23 2016, from https://en.wikipedia.org/wiki/Time-based_One-time_Password_Algorithm

[4] D. M'Raihi, S. Machani, M. Pei and J. Rydell, "TOTP: Time-Based One-Time Password Algorithm",RFC 6238, IETF, 2011. from https://tools.ietf.org/html/rfc6238

[5] RSA company, SecurId- from https://www.rsa.com/en-us/products-services/identity-access-management/securid

[6] A. Biryukov, J. Lano and B. Preneel, "Cryptanalysis of the Alleged SecurID Hash Function (extended version)" Lecture Notes in Computer Science, Springer-Verlag, 2003, 18 pages

[7] Patent US20140101043 A1- Sound-Based Payment Transactions. from https://www.google.com/patents/US20140101043

[8] R. Brown and L. Evans. Acoustics and the smartphone. In David J. Mee and Ian D.M. Hillock, editors, Proceedings of Acoustics 2011 — Breaking New Ground, Gold Coast, Australia, 2-4 November 2011. The Australian Acoustical Society, Queensland Division, 2011

[9] H. Lee, T. H. Kim, J. W. Choi, and S. Choi. Chirp Signal-Based Aerial Acoustic Communication for Smart Devices. In Proc. of IEEE Conf. on Computer Communications (INFOCOM), Hong Kong S.A.R., PRC, April 2015

[10] SimpleWebServer Java class, Android code samples, from https://developer.android.com/samples/PermissionRequest/src/com.example.android.permissionrequest/SimpleWebServer.html

[11] R. Sedgewick and K. Wayne, Princeton University, “Introduction to Programming in Java, a textbook for a first course in computer science”, FFT implementation class, from http://introcs.cs.princeton.edu/java/97data/FFT.java.html

[12] A simple Java OTP (One Time Password) generator library, currently supports RFC standard time based and counter based algorithms, GitHub repository, from https://github.com/kamranzafar/libotp

[13] R. Sedgewick and K. Wayne, Princeton University, “Introduction to Programming in Java, a textbook for a first course in computer science”, Complex Java class, from http://introcs.cs.princeton.edu/java/97data/Complex.java.html

[14] Josefsson, S. The Base16, Base32, and Base64 Data Encodings. RFC 4648, 2006. from http://tools.ietf.org/html/rfc4648

[15] Base64. In Wikipedia. Retrieved Nov. 23 2016, from https://en.wikipedia.org/wiki/Base64

[16] Low-pass filter. In Wikipedia. Retrieved Nov. 23 2016, from https://en.wikipedia.org/wiki/Low-pass_filter

[17] R. Nandakumar, K. K. Chintalapudi, V. Padmanabhan, and R. Venkatesan, “Dhwani: secure peer-to-peer acoustic NFC,” in Proc. ACM SIGCOMM, 2013, pp. 63–74

[18] J. Graham-Cumming, “Why some cryptographic keys are much smaller than others”, 20 Sep 2013. from https://blog.cloudflare.com/why-are-some-keys-small

[19] Orman, Hilarie, and P. Hoffman. "Determining strengths for public keys used for exchanging symmetric keys." (2004). RFC 3766. from https://tools.ietf.org/html/rfc3766

[20] Dujella and Andrej. "A variant of Wiener's attack on RSA." Computing 85.1 (2009): 77-83

[21] Lorraine, Inria, N. Loria, and F. Paul. "Factorization of a 512–bit RSA Modulus.". from http://www.iacr.org/archive/eurocrypt2000/1807/18070001-new.pdf

[22] M. Green, "A Few Thoughts on Cryptographic Engineering" blog, "Attack of the week: FREAK (or 'factoring the NSA for fun and profit')", March 3, 2015. from: https://blog.cryptographyengineering.com/2015/03/03/attack-of-week-freak-or-factoring-nsa

[23] HIS, Feb 2014. NFC-Enabled Cellphone Shipments to Soar Fourfold in Next Five Years. http://press.ihs.com/press-release/design-supply-chain/nfc-enabled-cellphone-shipments-soar-fourfold-next-five-years

[24] R. Nandakumar, K. K. Chintalapudi, V. Padmanabhan, and R. Venkatesan, "Dhwani: secure peer-to-peer acoustic NFC," in Proc. ACM SIGCOMM, 2013, pp. 63–74.

[25] Illiri- SAPI. http://www.zdnet.com/article/illiri-sound-api-aimed-at-secure-mobile-data-exchange-log-ins-payments

(*) הרפרנסים שעבורם מופיע הURL אינם רפרנסים אקדמיים לכן מובא הURL