Digital Whisper
Technologic Papers

על GSM, VoIP ומספרים חסויים

נכתב ע"י עדן משה (Devil Kide)

הקדמה

במהלך התקופה האחרונה יצא לי להתקל במספר אתרי אינטרנט שונים המציעים שרותי גילוי "שיחות חסומות". השרות מציע התקנת אפליקצייה מסויימת על ה-Smartphone אשר תגלה לנו בן רגע את פרטי הסורר. כאחד שבמהלך שרותו הצבאי היה חוקר פלילי, השרות נראה לי בתור עוד שיטה של נוכלים לעקוץ כסף מלקוחות תמימים. על מנת להבין כיצד תוכנות אלו פועלות יש צורך להכיר את הדרך שבה המכשיר הסלולארי שלנו פועל. במאמר זה אסקור את פרוטוקול GSM, שהוא למעשה אחד התקנים היותר נפוצים לתקשורת סלולארית.

איך הכל התחיל?

בתחילת שנות ה-80 החלה ההתפתחות במערכות הסלולאריות, דבר שגרם לגידול משמעותי בשימוש בטלפונים סלולארים. הואיל והעסק היה חדש יחסית, כל חברה סלולארית עבדה בצורה שונה מחברתה. באירופה ראו את הבעיתיות במחסור בתקן אחיד ולכן הוקמה ועדה שתפקידה היה לבחון מציאת טכנולוגיה אחידה למכשירים הסלולארים. טכנולוגיה שתקנה את אפשרות הנדידה עם אותו מכשיר סלולארי ממקום למקום, את ההפרדה בין זהות המכשיר לזהות המתקשר (SIM / IMEI) וגם הוזלה בעלויות המכשירים הסלולארים. התוצאה:

GSM - **G**lobal **S**ystem for **M**obile Communication

ללא כל צל של ספק, מדובר בפרוטוקול ישן ויש לו היום עשרות "שיפצורים", אך ה-GSM הוא היסוד של התקשורת הסלולארית, ועל כן אתמקד בו היום במאמר זה.

לפני הכל, מעט מושגים שחשוב לדעת

MSC / Switch (קיצור של Mobile Switching Center) - מרכזייה / מתג:

כחלק מתהליך התקשורת, חייבת להיות מרכזייה שתפקידה למעשה לנתב שיחות.

המרכזיה מחולקת ל-2 חלקים (סוגים?) שונים:

- **HLR (Home Location Registry)** - מרכזייה ביתית בה נמצא כל המידע על המשתמש ה"קבוע", וכך ניתן לזהות אם הוא משתמש בטיפול הרשת או שהוא אורח.

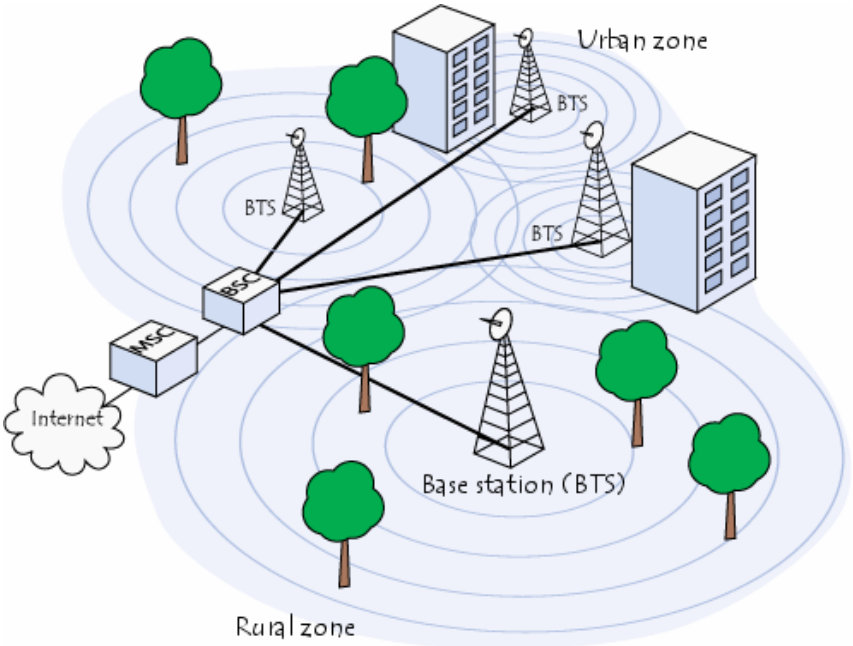
- **VLR (Visitor Location Registry)** - מרכזיה זמנית / מרכזיית מבקר. בזמן שמכשירכם לא נמצא תחת המרכזייה ה"ביתית" שלו, המכשיר יעבור לטיפול ה-VLR. לדוגמא, לעיתים כשנוסעים בסמוך לגבול , מתקבלת הודעה על כניסה לרשת מארחת.

תחת כל מרכזייה יהיו מספר תאים (Cell, מכאן גם מגיע השם "סלולארי"). לכל תחנה כזו, יהיה בקר (BSC) ומקלט (TRX):

- **BTS (Base Transceiver Station)** - תחנת הבסיס המשרתת את המנויים הסלולריים. כל תחנה מכילה מספר מסוים של משדרים / מקלטים.
- **BSC (Base Station Controller)** - תחנת הבקרה / בקר. רכיב שתפקידו להקצות למשתמשים תדרים על פי תדרים פנויים ועומסי רשת.
- **MSC (Mobile Switching Center)** - תחנות אשר תפקידן קבלת שיחות ולמקם אותן ברשת, תפקידן לתשאל את רכיבי ה-HLR ולנתב את השיחות אל יעדן.
- **OMC (Operation and Maintenance Center)** - מרכז התפעול והתחזוקה, ה"לוגים" של השרת, המקום בו נרשמות כל התקלות בעת הביצוע.
- **EIR (Equipment Id Registr)** - רכיב זה משמש לצורך ניהול המכשירים עצמם (IMEI) כשהשימוש העיקרי שלו הוא טיפול במכשירים גנובים. ל-EIR יהיו שלושה רשומות:
  - ✓ רשומה לבנה - מכשיר תקין.
  - ✓ רשומה שחורה - מכשיר גנוב שאין לתת לו שרות.
  - ✓ רשומה אפורה - מכשיר שצריך לעקוב אחריו.
- **AUC (AuthenticationCenter)** - מערכת שמטרתה לטפל בזיהוי המחמיר. המערכת בודקת שה-SIM שמנסה להתחבר לרשת, תקין ועומד בדרישות.
- **SM (Mobile Station)** - משתמש הקצה, המכשיר הסלולארי.
- **SIM (Subscriber Identity Module)** - כרטיס חכם המכיל את נתוני הזיהוי של המנוי ומידע הדרוש לצורך הצפנת השיחה.
- **IMSI (International Mobile Subscruber Identity)** - קוד זיהוי חד-חד ערכי, המאפשר זיהוי המשתמש ברשת. לרוב הקוד יורכב מ-15 ספרות, כאשר שלושת הספרות הראשונות יצגו את מדינת ה"בית" של המכשיר, 2-3 ספרות הן קוד הרשת והשאר הספרות הן מספר MSIN.
- **IMEI (International Mobile Equipment Identity)** - מספר הזהות של המכשיר הסלולארי שלנו (בכדי לגלות את מס' ה-IMEI ניתן להקיש, משמאל לימין, בכל מכשיר סלולארי את הצירוף #06#*).

- **TSC (transit switching center)** - השער האחרון לפני המעבר לרשתות אחרות (בין אם רשת נייחת ובין אם רשת ניידת).
- **VoIP (Voice over IP)** - משפחה(?) של פרוטוקולים אשר תפקידם להעביר שמע או וידאו דרך רשתות מבוססות IP, פרוטוקולים לדוגמא: SIP ו-IAX.
- **SIP (Session Initiation Protocol)** - פרוטוקול בשכבת האפליקציה, תפקידו לנהל שיחה קולית / וידאועל ידי ניהול הפרוטוקול, על גביו מועברות חבילות המידע (כדוגמאת הפרוטוקול RTP), SIP הינו פרוטוקול טקסטואלי וקריא, המזכיר במבנה שלו את הפרוטוקול HTTP המוכר לנו.
- **Asterisk** - מערכת מרכזיית IP, מבוססת תוכנת קוד פתוח. בין השאר נותנת שרות Voice over IP, ללא תוספת של חומרה מיוחדת. המערכת רצה על כל סוגי מערכות ההפעלה, אולם מומלץ להריץ אותה על מערכות הפעלה לינוקסאיות.

כל הרכיבים המפורטים לעיל הם למעשה הכלים העיקריים והמרכזיים שמרכיבים את המערכת איתה עובד הטלפון הסלולארי שלנו, או כל מכשיר שמשתמש ב-GSM, מהאנטנה עד למשתמש הקצה. אם נסתכל החוצה,לדוגמא אל החצר שלנו, נוכל לבחון מקרוב את מבנה המערכת. הדבר יראה בערך כך:



[במקור: http://www.techviral.com/telecom/gsm-network-works]

אולם, איך כל המערכות האלה מקנות לנו את היכולת להעברת מידע בצורה כל כך מהירה ומדוייקת, עם יכולת נדידה וכל זאת מבלי שנרגיש הפרעות בשיחה?

אז איך זה עובד?

נתמקד מעט בטכנולוגיה הנקראת GSM. GSM, ראשי תיבות של: **G**lobal **S**ystem for **M**obile-Communication הינו תקן לרשתות תקשורת סלולאריות (הוא מוגדר כ-"דור שני" מפני שאופן תעבורת השמע הינה דיגיטלית). עמדות הקצה (לקוחות הרשת) מכונות "Mobile Station". כאשר עמדה A מעוניינת ליזום שיחה עם עמדה B:

- ראשית, מתבצעת בקשת התחברות לרשת. עמדת הקצה מזהה את רכיב ה-BTS (Base Transceiver Station), אנטנות המפוזרות ברחבי העיר, ושולחת דרכו בקשת התחברות מצורפת בנתונים על המכשיר ועל מזהיו.

- הבקשה נשלחת מעמדת הקצה דרך רכיב ה-BTS ומגיעה ל-BSC (Base Station Controller) תחנות בקרה ברשת.

- תחנות הבקרה מעבירות את המידע ליחידות ה-MSC (Mobile Switching Center) ולעמדות ה-OMC (Operation and Maintenance Center) שבהן יאגר מידע כגון תקלות ו-Metadata על השיחה.

- בעת קבלת בקשת ההתחברות לרשת, תחנות ה-MSC אחראיות לתשאול יחידות ה-HLR, בהן מאוחסן המידע על יחידת ה-MS, על איפיון המכשיר כגנוב או לא. במידה והכל כשורה - האירוע נרשם ונשלח ליחידת הקצה לאישור התחברות לרשת עם הפרטים הנדרשים.

- כעת, לאחר קבלת פרטי האישור, תחנה A מסוגלת ליזום שיחה ליעד B. כאשר תחנה A מבקשת ליזום את השיחה עם תחנה B, הבקשה מועברת לתחנת ה-MSC (דרך יחידת ה-BTS), ותפקיד תחנת ה-MSC, הוא תשאול תחנת ה-HLR ולברר תחת איזו תחנת MSC נמצאת הרשומה של לקוח B בזמן הנתון. בזמן תשאול תחנת ה-HLR, תחנת ה-MSC אחראית להחזיר ללקוח A צליל המתנה.

- לאחר קבלת פרטי תחנת ה-MSC המשרתת את לקוח B, תחנת ה-MSC של לקוח A יוצרת פנייה לתחנת ה-MSC ומבקשת ממנה לאתר את תחנת ה-BSC המקושרת ללקוח B, תחנת ה-BSC מאתרת את יחידת ה-BTS שמשרתת באותו הרגע את לקוח B ודרכה שולחת לו את הבקשה של A ליצירת השיחה.

טווח התדרים הסטנדרטי ברמת העלאת המידע שלנו לשרת (UpLink) יהיה בין 890 ל-915 מגה-הרץ (אולם טווח זה עשוי להשתנות ממדינה למדינה), לעומת זאת,טווח קבלת המידע מהשרת (DownLink) יעמוד על 935-960 מגה הרץ.

בהתייחסות עדינה לנושא הניצול המירבי של יכולות הרשת נבחן בקצרה את FDMA, ואת ההשתלשלויות שלו, ה-TDMA או ה-CDMA: בתחילת שנותיו של עולם הסלולאר הרשתות היו אנלוגיות והטכנולוגיה בה השתמשו לשם חלוקת התדרים הייתה ה-FDMA.

הרעיון היה פשוט, לוקחים את טווח התדרים העומד לרשותינו ומחלקים אותו לערוצי רדיו צרים, כך שכל משתמש מקבל ערוץ בלעדי לשם ביצוע שיחה. בנתיב הזה מעביר המשתמש את האינפורמציה הדרושה בנתיב הלוך (UpLink) ובנתיב החזור (DownLink). רוחב הפס עמד על כ-30KHz. לאחר תקופה קצרה התברר שהגישה הזו מאוד בעייתית, מבחינת זמינות המשאבים ובטחון מידע (לדוגמא, בעזרת מקלט פשוט ניתן היה להאזין לשיחות).

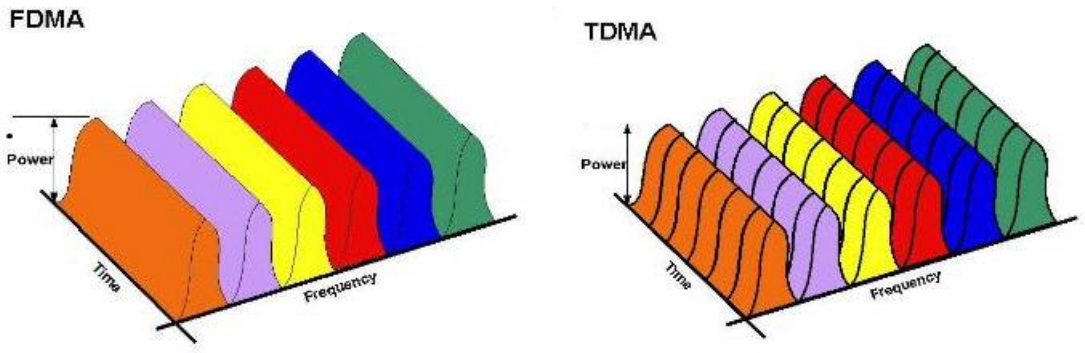
לאחר שה-FDMA התגלתה כתקשורת מעט בעייתית הטכנולוגיה פינתה את מקומה לטכנולוגיות מתקדמות קצת יותר כמו ה-TDMA, אשר הכניסה לתוכה בצורה יוצאת דופן את נושא השימוש במשאבי הרדיו המוגבלים (למעשה, עד היום היא נחשבת כיעילה).

הרעיון הבסיסי הוא לחלק את תדר הרדיו למשבצות זמן עוקבות (Time Slot). כל משתמש מקבל משבצת זמן כזו, כך שניתן לנצל את אותו תדר רדיו למספר משתמשים שונים. לצורך ייעול השיטה, כל שתי משבצות מרכיבות שיחה אחת, כך שמשבצת אחת מהווה את נתיב ההלוך והמשבצת השנייה מהווה את נתיב החזור. כיום, רשתות ה-GSM משתמשות בטכנולוגית ה-TDMA לשם חלוקת משאבי המערכת.

בנוסף ל-TDMA קיימת שיטה שלישית לחולקת המידע, ה-CDMA, ששונה מהטכנולוגיות הקודמות בצורה מאוד משמעותית. הטכנולוגיה אינה משתמשת במשבצות זמן או בתדרים שונים, אלא מפזרת את אותות הרדיו על פני טווח תדרים רחב ביותר (רחב הרבה יותר ממה שנדרש כדי להפיץ את המידע).

לצורך ההדגמה, שיחה קולית דורשת רוחב פס של 8KHz, אך עם המערכת היא תופץ על פני רוחב פס של 1.5KHz או יותר.

בכדי לא לבזבז משאבים, ניתן לשלב מספר גדול של שדרים על גבי אותו תדר ולהבדיל בין אותות השיחה השונים באמצעות קידודים של השיחה. שנית, בשל שליחת המידע בעוצמה על גבי רוחב פס גדול מאוד ישנה הגנה מפני מכשולים, המפחיתים מן האנרגיה של האות. בנוסף, השימוש ב-CDMA מקנה את הביטחון שלכאורה אף אחד אינו יכול לאתר את התדרים בהם משתמש הקצה משדר ובכך הטכנולוגיה מגבירה את פרטיות השיחה.



[FDMA אל מול ה-TDMA. נלקח מ-Rynacomm.net]

כאחד מעקרונות היסוד של מערכת תקשורת תאית היא האפשרות לחלק את ערוצי השיחה שלנו לשימוש חוזר, כך שכל תדר יכול לתת שרות ליותר ממשתמש קצה אחד, בתנאי שהתאים מספיק רחוקים, מה שמקנה לכל MSC את היכולת לתמוך בסדר גודל של כ-100,000 מנויים וכ-5,000 שיחות.

על סמך המידע הזה, ניתן להבין את הצורה בה חברות הסלולאר ממקמות את תחנות הבסיס (BTS) שהן מפעילות, קרי, תחנות הבסיס מחולקות על סמך הטופוגרפיה של המקום ועל סמך ריבוי המשתמשים באיזורים מסויימים. לדוגמא בסמוך לקניון מרכזי או איזור הומה אדם תוצב יותר מתחנת בסיס אחת בכדי לתת לכלל המשתמשים את השרות המקסימלי. מה שיכול לקרות הוא ששני אנשים שנמצאים אחד בסמוך לשני יקבלו שרות, מ-BTS שונה. המכשיר הסלולארי "יבחר" את את תחנת הבסיס המתאימה לו ביותר על סמך התחנה עם הכי פחות עומס, שנותנת את הקליטה הגבוהה ביותר.

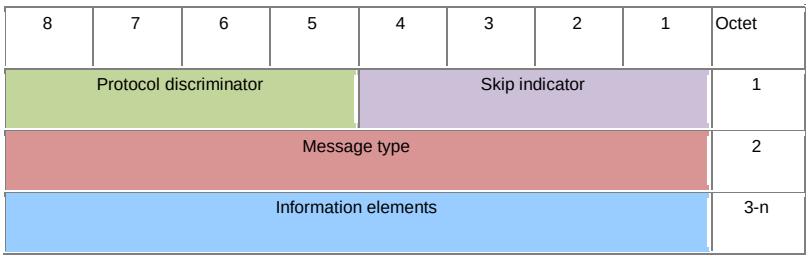
משתמש הקצה, יוצג כרגע כמכשיר סלולארי המנהל מערכת יחסים מאוד מרוכבת עם הרשת של החברה המפעילה, שולח אות המאפשר לרשת לזהות אותו, ועל סמך מידע זה הרשת תדע להפנות שיחות אל המשתמש בכל מקום בו יימצא, מהרגע שהמכשיר מופעל וכל פרק זמן קצר שולח המכשיר הסלולארי "אות חיים", שמעיד על כך שהמכשיר דולק, מיקומו ופרטים נוספים.

בעת הפעלת המכשיר נשלחת בקשת התחברות ביחד עם נקודת המיקום שלנו, סוג המכשיר, מספר ה-SIM ומספר ה-IMEI אל ה-BSC, אשר מעביר את הבקשה אל ה-MSC, שפונה אל ה-HLR לשם אישור בקשת ההתחברותווידוא כי המכשיר נמצא ברשת הביתית שלו, (במקביל מתבצעת בדיקה אל מול הרשימות השחורות / אפורות / לבנות), ה-HLR מאשר את הבקשה ומוסיף למאגר את המיקום הנוכחי של המכשיר הסלולארי.

במרחב הגאוגרפי קיימות שתי מערכות עיקריות, שבעזרתן מתבצעות שיחות קוליות, שליחת הודעות MMS או כל מידע אחר שהוא לא קולי:

- **Circuit Switch** - מערכת מיתוג המעגלים המשמשת למשלוח תעבורה קולית.
- **Packet Switch** - מערכת מיתוג מנות, המשמשת למשלוח מנות מידע אל האינטרנט או הודעות MMS.

המכשיר הסלולארי שולח את המידע בדיוק כמו המחשב שלנו- בצורת ביטים שהרשת או כל מי שמקבל את המידע, ידע לפענח אותו ולהבין אם מדובר בבקשה ליצירת שיחה, דחיית בקש או אימות בקשה. הבקשות נראות כך:



[במקור: http://www.protocols.com/pbook/umtsfamily.htm]

כאשר ביט 8 שמור בעתיד להרחבה. ביט 7 נשמר לזיהוי הרציף להודעות הנשלחות מתחנה ניידת.

מבנה חבילת המידע ב-GSM, ערך **Protocol discriminator** יהיה הערך הבינארי 1010, ו**מזהה הדילוג** יהיה 0000. **סוג ההודעה** יכיל מידע שיזהה באופן חד-ערכי את הבקשה או את הפעולה שצריכה להתבצע.

סוגי הודעות ב-GSM:

מזהה	תפקיד
01XXXXXX	הודעות ניהול שיחה
1000001	הפעלת בקשת הקשר PDP
1000010	הפעלת אישור הקשר PDP
1000011	הפעלת דחית הקשר PDP
1000100	בקשת הפעלת הקשר PDP
1000101	דחיית בקשת הפעלת הקשר PDP
1000110	ביטול הפעלת בקשת הקשר PDP
1000111	ביטול הפעלת בקשת הקשר PDP
1001000	אימות בקשת הקשר PDP
1001001	אימות אישור הקשר PDP
1010000	הפעלת בקשת הקשר AA PDP

1010001	הפעלת אישור הקשר AA PDP
1010010	הפעלת דחיית הקשר AA PDP
1010011	ביטול הפעלת בקשת הקשר AA PDP
1010100	ביטול הפעלת אישור הקשר AA PDP
1010101	מצב SM

כל הנתונים הנ"ל משתנים בין פרוטוקול לפרוטוקול, ניתן לקרוא עוד על נתוני החבילה בפרוטוקולי סלולאר שונים בקישור הבא:

http://www.protocols.com/pbook/pdf/cellular.pdf

בעת ביצוע כל פעולה המכשיר שולח מס' חבילות מידע הכוללות כותרים (Headers) שונים.

המכשיר הסלולארי שלנו שולח עשרות רבות של חבילות מידע, כשכל אחת מכילה בתוכה פיסות מידע שונות. ניתן לראות כאן את הרשימה המפורטת של ההדרים הנשלחים. מומלץ, לכל הפחות, לעבור ברפרוף על האתר הזה ובייחוד על "P-Asserted-Identity".

קיימות פרצות רבות המתבססות על בעיות ברשת ה-GSM, הנושא הזה הוא עולם ומלואו ובכדי להבין עד כמה אנחנו חשופים לכל כך הרבה בעיות כשאנחנו משתמשים במכשיר סלולארי (ובמקרים מסויימים, אפילו שהמכשיר **לא בשיחה**) מומלץ לקרוא עוד בנושא.

על מנת לברר מי התקשר אלינו ממספר חסום יש צורך בצו חתום ע"י בית משפט ומומלץ סיוע של אחת הרשויות החוקרות. שמא קיימת דרך אחרת? כאן נכנסת לתמונה מערכת טלפוניה מבוססת קוד פתוח הנקראת Asterisk, המערכת נותנת שירות לשיחות מבוססות IP (Voice Over IP) ולשיחות טלפון רגילות המוכרות לנו.

קצת על Asterisk

קיימות מספר גרסאות למקור השם אסטריסק.אחד מקורות השם הינו התו '*' - מקש שנמצא על לוח המקשים ובעל יכולת לבצע פעולות מיוחדות. והיותו תו מיוחד במערכות UNIX. הדרך הנכונה לשלוט על מערכות אסטריסק הוא תכנות / קינפוג ה-DailPlan שלה- משמע להורות למערכת מה לבצע כתגובה לכל פעולה שמתבצעת. ישנם מספר דרכים לדבר עם המערכת; האחת, שפת תכנות ששמה AEL; האפשרות הנוספת הינה דרך ממשק AGI

(קיצור של Asterisk Gateway Interface), תוכנית חיצונית המתקשרת עם המערכת באמצעות קלט / פלט סטנדארטי.ניתן לעבוד עם המערכת כמו שהיא, למשתמש הפשוט קיימים מספר ממשקי ניהול שדרכם ניתן לשלוט על המערכתובכך יכולים להקל על עבודתו, אך חשוב לזכור כי לעיתים הממשקים מוגבלים ומגבילים. שני ממשקים מוכרים הם Asterisk-GUI - הממשק שמפותח ע"י Digium, החברה שמפתחת גם את המערכת עצמה ו-FreePBX. בנוסף לכך, קיימות מספר "הפצות "Asterisk כגון Trixbox, AsteriskNOW, Elastix ועוד.

במקביל ל-Asterisk קיימות עוד עשרות מערכות טלפונייה שונות ומגוונות, חלקן של חברות מוכרות יותר כמו פנסוניק וארִיקסון. עדיף להשתמש באסטריסק הן בשל העלויות הזולות והנגישות והן בגלל הגמישות המאוד גבוהה של המערכת. Asterisk מספקת (ע"פ רוב) שרות טלפוני לעסקים, אפשרות ליצור מערכת ניתוב שיחות, אפשרות למספר רב-קווי, מערכות קול אינטראקטיביות, מערכת לניהול תורי שיחות וכו'.

קצת על SIP

SIP (קיצור של Session Initiation Protocol, RFC מספר 3261), הינו פרוטוקול בתצורת שרת-לקוח בשכבת האפליקציה. בדרך כלל המידע מועבר על גבי UDP בפורט 5060, אך אין שום בעיה להשתמש בו גם מעל TCP, ובכל פורמט אחר. תצורתו מזכירה מאוד את המבנה של HTTP, הן מפני שמדובר בפרוטוקול קריא והן מפני שמספרי ההודעות בפרוטוקול דומות ברובן למספור ההודעות ב-HTTP (כדוגמאת 4XX - הודעות שגיאה, 3XX - העברת השיחה, 2XX - הודעות להצלחה וכו') , דבר המקל על העבודה איתו.

דוגמאות להודעות הקיימות בפרוטוקול (נלקח מהמאמר PenTesting VoIP, שנכתב על ידי שי רוד ופורסם בגליון ה-20 של Digital Whisper):

בקשה	תיאור
INVITE	משמשת להזמנת חשבון להשתתף בשיחה.
ACK	אישור על קבלת הזמנה להשתתף בשיחה.
CANCEL	ביטול בקשה ממתינה.
REGISTER	רישום משתמש מול שרת SIP.

OPTIONS	מציג רשימת יכולות הקיימות אצל המתקשר.
BYE	ניתוק שיחה בין שני משתמשים.
REFER	מציין כי הנמען (מזוהה באמצעות בקשת URI) צריך לתקשר דרך צד שלישי באמצעות מידע המסופק בבקשה.
SUBSCRIBE	משמשת לשליחת בקשה לקבלת המצב הנוכחי של השירות ומצב העדכונים משרת מרוחק.
NOTIFY	מודיע לשרת SIP כי אירוע אשר התבקש ע"י בקשת SUBSCRIBE קודמת התבצע.

דוגמאות לבקשות כאלו נראה בהמשך.

איך כל זה מסייע לנו? המערכת מהווה מעיין נקודה חכמה בין המערכת הסלולארית לבין רשת הטלפון הפרטית שלנו, המערכת יכולה לפעול על כל מחשב, דבר שנותן לנו מעט שליטה על המערכת ועל הנתונים שהיא מקבלת. בעת הקמת שיחה קולית המכשיר שולח HEADER's מסויים. בהוצאת השיחה נשלח HEADER המכיל, בין השאר את השדה P-Asserted-Identity, המכיל בתוכו את מספר הטלפון של יוזם השיחה. P-Asserted-Identity הינו למעשה ה-Header האחראי על זהות השיחה.

ה-P-Asserted-identity משמש גופים מהימנים (בד"כ לרכיבים המתווכים) לצורך זהות המשתמש. בנוסף לשדה הזה נשלח דגל שמורה האם להציג את מספר הטלפון של מחייג השיחה או להשאיר אותו מוסתר מעיני מקבל השיחה. כלומר, בכל מצב ה-PAI יכיל בתוכו את מספר הטלפון של מחייג השיחה והשאלה אם נראה את המספר תלויה בדגל מסויים - נשאלת השאלה איך נוכל לשנות את הדגל, או לחלופין להגיע למספר הטלפון?

המכשירים הסלולארים שלנו מאוד מוגבלים, אולם מה יקרה אם תהיה לנו שליטה על המידע שזורם בין הרשת למכשיר הסלולארי? וכאן בדיוק נכנסת מערכת ה-Asterisk.

במכשירים סלולארים קיימת אפשרות ניתוב שיחה; במצב של חוסר מענה / ניתוק השיחה נוכל להגדיר כי השיחה תועבר באופן אוטומטי למספר טלפון אחר (השרות הזה מוכר בד"כ במכשירים הקבועים ברכב ובמצב שהמשתמש לא עונה השיחה תעבור ישירות למכשיר הנייד).

ניתן להעביר כל שיחה ממספר חסום אל שרת האסטריסק שלנו, שיבצע ניתוח של המידע ויחזיר אלינו את השיחה תוך שהוא חושף את ה-CallerID עבורנו. על מנת להעביר שיחות מבלי להעזר בתפריט המכשיר ניתן להעזר בחיוג המספרים הבאים (נכון לרשת אורנג', לא נבדק ברשתות אחרות):

מספר	תכונה
21	כל השיחות ללא תנאי
61	באין מענה
62	כאשר כבוי\לא זמין
67	כאשר תפוס

השרות יתבצע בצורה הבאה (מימין לשמאל): ***קוד הפנייה*טלפון להעברה#.**

בכדי שאסטריסק תדע לנתח את המידע צריך לקנפג את השרת וללמד אותו לעשות זאת. קווין מיטניק הרצה על הנושא בכנס HOPE, מיטניק העלה את הנושא (להרצאה המלאה, מומלץ בחום) ואף הדגים כיצד הוא מגלה את מספר הטלפון של מי שמתקשר ממספר חסום.

אז איך זה נראה? (**הדוגמאות לקוחות מהרצאה של מיטינק** - בדוגמה הנ"ל השימוש הוא בחברת Flowroute לקישוריות). כאשר נכנסת שיחה **רגילה**, חבילת המידע נראית כך:

```
INVITE sip:12089682000@[removed] SIP/2.0
(...)
From: <sip:+18053414555@70.167.153.130>;tag=20bc14f6bc...
To: <sip:+12089068200@70.167.153.130>
Call-ID: 1214297526-7946826@LA4_SIP_01
CSeq: 200 INVITE
Contact: Anonymous <sip:70.167.153.135:5060>
P-Asserted-Identify: <sip:+18053414555@sip.flowroute.com>
(...)
```

ניתן לראות כי מדובר בבקשת "INVITE", הזמנה לשיחה. ניתן לראות כי הכותר "From" מעביר לנו את מספר יוזם השיחה. בנוסף ניתן לראות כי אותו מספר בדיוק נשמר גם בכותר "P-Asserted-Identify".

כאשר נכנסת שיחה **חסויה**, חבילת המידע נראת כך:

```
INVITE sip:12089682000@[removed] SIP/2.0
(...)
From: <sip:anonymous@70.167.153.130>;tag=de2b0ed15264…
To: <sip:+12089068200@70.167.153.130>
Call-ID: 1214297526-7946826@LA4_SIP_01
CSeq: 200 INVITE
Contact: Anonymous <sip:70.167.153.135:5060>
P-Asserted-Identify: <sip:+18053414555@sip.flowroute.com>
Privacy: Id
(...)
```

במקרה זה ניתן לראות כי כאשר נכנסת שיחה המוגדרת כחסויה, שדה ה-From אינו מכיל את מספר יוזם השיחה, ובנוסף לכך ניתן לראות כי נוסף לנו כותר נוסף "Privacy". עם זאת, ניתן לראות כי הכותר P-Asserted-Identify עדיין מחזיק את מספר יוזם השיחה. מה שאומר שכאשר מתקשרים אלינו ממספר חסוי, הצד השני עדיין מקבל את מספר יוזם השיחה, אך הוא יודע לא להציג אותו למשתמש!

מיטניק הציע את התגובה הבאה: נעביר את כלל השיחות דרך מרכזיית VoIP. כאשר נקבלה שיחה חדשה, המרכזיה תבדוק האם מדובר בשיחה חסויה. במידה ומדובר בשיחה שאינה חסויה- היא תעבור כרגיל למכשיר שלנו, במידה ואכן מדובר בשיחה חסויה – המרכזיה תדע לערוך את חבילת המידע (להשמיט את הכותר "Privacy", ולשכתב את הכותר "From" עם הערך הקיים ב-"P-Asserted-Identify", מה שיגרום לכך שגם אם נקבל שיחה ממספר חסוי - נוכל לדעת מה המספר המקורי.

ברמת הפרטיקה הוא פרסם מספר שורות שצריך להוסיף ל-extensions.conf על מנת לסייע לנו עם גילוי המספר המוסתר. לשם הידע, extensions.conf זהו קובץ קונפיגרציה האחראי על הרחבות במערכת אסטריסק (מיקום הקובץ: /etc/asterisk/).

phant0msignal, העומד מאחורי הבלוג "Tracing The Signal" פרסם את השורות שמיטניק כתב עבור extensions.conf בתוספת הסבר:

```
[inbound]
;For Asterisk 1.4

;workaround to prevent rtp deadlock
exten => YOURSIPNUM,1,Playback(silence/1|noanswer)
;save the callerid to a variable
exten => YOURSIPNUM,2,Set(passertedid=${SIP_HEADER(P-Asserted-
Identity)})
;save the privacy bit to a variable (if it is set)
exten => YOURSIPNUM,3,Set(privheader=${SIP_HEADER(Privacy)})

;check if callerid is private
exten => YOURSIPNUM,4,GotoIf($[${LEN(${privheader})} > 1]?8)

;send out regular callerids without modification
exten => YOURSIPNUM,5,Set(CALLERID(all)=${CUT(passertedid,@,1):5})
exten => YOURSIPNUM,6,Dial(SIP/YOURPHONEMUN@flowroute)

;prepend 900 to blocked callerids before unmasking
exten => YOURSIPNUM,8,Set(CALLERID(all)=+900${CUT(passertedid,@,1):5})
exten => YOURSIPNUM,9,Dial(SIP/YOURPHONEMUN@flowroute)
```

יש להחליף את YOURPHONEMUN למספר טלפון שלך, אליו אתה רוצה להעביר את השיחות. את המספר YOURSIPNUM יש לשנות עם מספר ה-VOIP שרכשת.

חשוב לציין כי חברות הסלולאר בארץ עוטפות את המידע העובר ב-PAI, ככה שייתכן שבמקום לקבל את המספר של מחייג השיחה נקבל מספר מפוברק. על מנת להתגבר על בעיה זו ניתן לקנות חשבון SIP זר שידוע לנו שאינו "מטפל" ב-HEADER's האחראיים על הסתרת מספר המתקשר.

סיכום

אין ספק שאנו נמצאים בעידן חדש, דור ה"אייפון", תקופה שבה אנחנו מבצעים כל פעולה דרך המכשיר הסלולארי החכם שלנו. יש שיסכימו איתי שהמחשב הביתי נהיה נחלת העבר אל מול המכשירים הסלולארים שיכולים להריץ אפליקציות מתוחכמות העשירות בגרפיקה ובביצועים. אולם עם כל הטכנולוגיה הזו אנו עדיין עובדים אל מול רשת ה-GSM, שמקנה לנו את היכולת לבצע שיחות קוליות או להעביר מידע בקלות וללא כל בעיה.

הרשת עובדת על גלי רדיו במספר שיטות וצורות, הטכנולוגיה של ה-GSM עברה מספר שדרוגים וגלגולים, אולם עם כל זאת ראינו שנושא הבטחון מידע אינו בראש סדר העדיפויות של החברות הסלולאריות. על מנת לאתר שיחות ממספר חסוי אנחנו לא צריכים יותר ממחשב ביתי פשוט עם יכולות תמיכה ב-VOIP, מעט ידע והמון מצב רוח.

קישורים מומלצים

- איך לחשוף שיחה מזוהה
- Caller ID Spoofing - rootSecure
- How GSM works - scribd
- כל ה-HEADERS הנשלחים ברשת GSM
- ההרצאה של קווין מטניק בנושא
- אתר הבית של Asterisk
- http://ccnga.uwaterloo.ca/~jscouria/GSM/gsmreport.html
- http://phant0msignal.blogspot.com
- http://www.voip-info.org
- http://www.digitalwhisper.co.il/files/Zines/0x14/DW20-2-PenTest-VoIP.pdf

הערה

אין כותב מהמאמר אחראי על התוכן, כל המידע הכתוב כאן קיים ונמצא ברשת האינטרנט. כותב המאמר אינו ניסה את כל הכתוב במאמר ואינו מעודד לנסות את כל הכתוב בו.

שלכם,

עדן משה / Devil kide.