3G Mobile Network Security

מאת רועי חורב (AGNil)

מבוא למבוא

לא מזמן התעוררתי. אפילו לא שמתי לב שישנתי כל כך הרבה, ובזמן שאני ישן לי שנת ישרים (המומחיות שלי), כל העולם מסביבי התפתח והתקדם לו. עד לפני כמעט חודש, השתמשתי במכשיר הסלולארי שלי ככלי לתקשורת מילולית. היו לי כמה וכמה מכשירים, חלקם היו מתוחכמים יותר וחלקם מתוחכמים פחות- אבל העניין הסתכם בזה שכולם התמקדו בביצוע שיחות ובשליחת SMS-ים. הבאזז שחברת Apple יצרו עם מכשיר ה-iPhone שלהם, הצליח איכשהו לפסוח עליי. האמת היא שאני יודע טוב מאוד למה, אבל כדי לחסוך לי 15,000 תגובות נזעמות של חסידי המכשיר, אני לא אשתף אתכם בסיבות המדויקות. ופתאום, ללא שום אזהרה מוקדמת, החלטתי לקנות לעצמי מכשיר סלולארי חדש. אחוז תזזית התיישבתי ליד המחשב, פתחתי Google והתחלתי לחפש מכשיר שכזה . אם כותבים את המילה "Phone" ב-Google, התוצאה הראשונה מפנה כמובן ל-iPhone, אבל התוצאה האחרונה הפנתה לטלפון של Google. אחרי תחקיר מהיר, החלטתי להשקיע את כספי דווקא במכשיר הפחות מוכר הזה. אני בטוח שחלקכם מעקמים עכשיו את האף ואומרים לעצמם: "איזה דגנרט מתעסק באבטחת מידע בחיי היום-יום, והולך וקונה טלפון של Google?!" התשובה היא פשוטה. אני. המכשיר רץ על פלטפורמה פתוחה בשם Android, מבוססת לינוקס, שבהחלט מסוגלת לספק את הכלים להחליט איזה מידע אני כן רוצה לשתף עם המפלצת, ואיזה מידע פחות. בכדי לקצר את כל הסיפור המפרך הזה , ושוב, בניסיון נואש להתחמק מדיונים שמאוד קשה לצאת מהם אחר כך, קניתי שלושה מכשירי NEXUS1 מבית היוצר של HTC, תחת האבא התומך Google. המכשירים הגיעו, אחד אליי, ושניים לחברים שנדבקו מההתלהבות שלי – ואני התחברתי שוב אל קדמת הטכנולוגיה, שזנחה אותי מאחור מבלי להוציא מילה.

המכשיר עצמו מדהים. מצאתי עצמי מהר מאוד זונח את המחשב הנייד במספר רב של מקרים, ומשתמש רק בסלולארי על מנת לקרוא מיילים, לגלוש, לסנכרן מידע ועוד.

הפעולות האלה שמצאתי את עצמי עושה גרמו לי לעצור רגע ולתהות בכל מיני שאלות – האם אני גולש ועובד תחת חיבור מאובטח? האם גורמים ואנשים אחרים יכולים להאזין לתעבורת התקשורת שלי? האם אני יכול להאזין לתעבורה של אנשים אחרים? האם המידע על המכשיר עצמו מאובטח?

בדרך כלל כשאני נכנס לאינטרנט, אני מודע (ברמה כזו או אחרת) למיליון הסכנות שאורבות לי, ומשתדל "לנהוג בהתאם לתנאי הדרך". ופתאום, אני מחובר לאותה רשת – עושה את אותם פעולות, וזאת מבלי לדעת מי או מה יכול לקרות לי בדרך. מטריד.

קצת רקע

לפני שנכנס לדיוני אבטחת מידע ברומו של עולם, חשבתי לשפוך קצת רקע על מה זה בעצם החיה הזאת שנקראת "דור שלישי". בפעם הראשונה ששמעתי את המושג "דור שלישי" חשבתי שמדובר על ספירת הדורות מאז הנאצים יימח שמם, וזה גם הסתדר כרונולוגית – אבל משמעות המושג רחוקה מכך, וחשוב להבין מה כל זה אומר.

ובכן דור שלישי זה אינו השם של הטכנולוגיה, אם כי יותר שם שיווקי, שמעיד על יכולות תקשורת מהירות יותר. החלוקה בצורה גסה מאוד מתחלקת כדלקמן:

1. "דור ראשון" – תקשורת סלולארית אנלוגית – התחילה איפשהו בתחילת שנות ה- 70. המטרה הייתה להעביר שיחות בלבד, אך כבר אז התחילו להשתמש במכשיר כמודם. המהירות שהצליחו לסחוט מזה, לא הייתה הרבה מעבר ל-10Kbps.

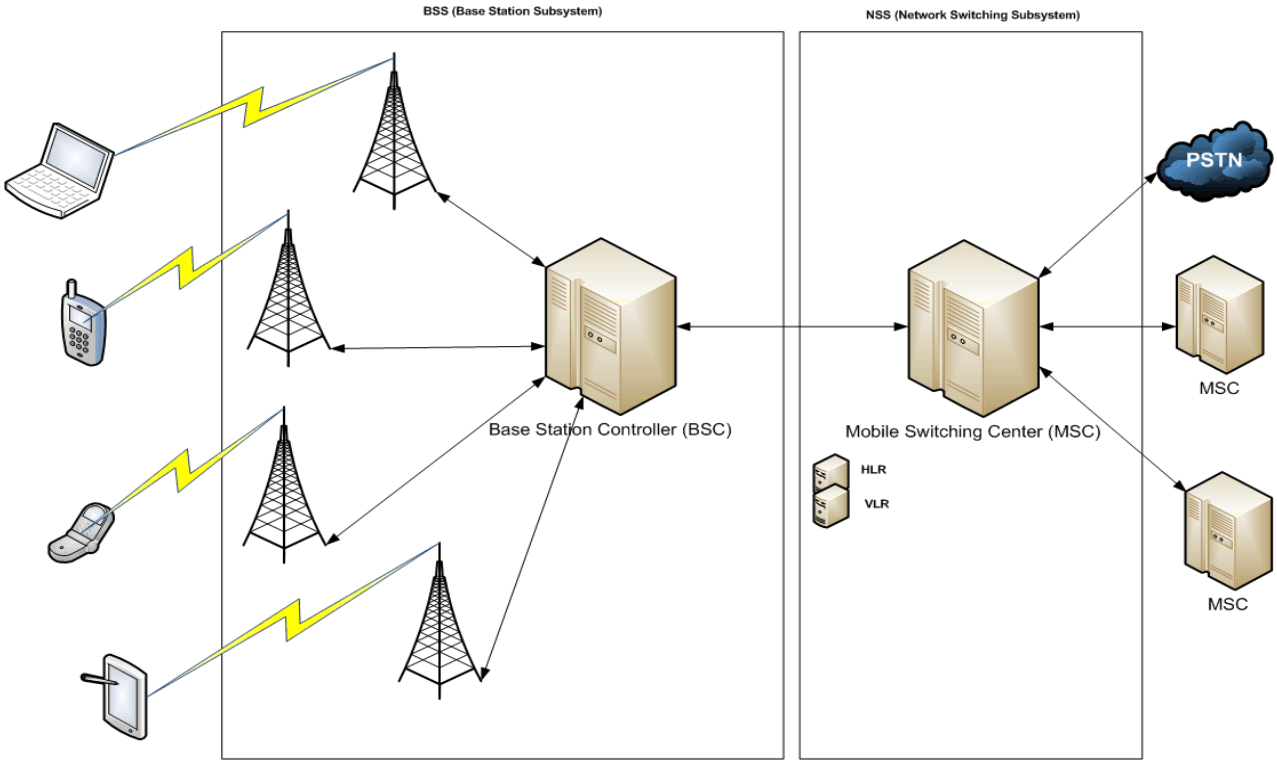
2. "דור שני" – תקשורת סלולארית דיגיטלית – התחילה את דרכה בשנות ה-90. היא התבססה של שלוש טכנולוגיות תקשורת שונות: GSM, CDMA, ו-TDMA.
"דור שני וחצי" הכניס למשוואה את חבילות ה- DATA שכללו בין היתר גישה לאינטרנט, דוא"ל והורדות במהירות של עד 200 Kbps.

3. "דור שלישי" – התפתחות נרחבת של הרשת לתמיכה ביותר משתמשים על כל מערכת, והגברת מהירות האינטרנט עד לכ- 1Mbps. בנוסף, הדור השלישי מאפשר יכולת "נדידה גלובאלית" של המכשיר, מה שאומר שאפשר לעבור בין רשתות GSM לרשתות Wireless. רשתות 3g של GSM נקראות WCDMA ו-HSPA, והרשת של CDMA נקראת CDMA2000.

4. "דור רביעי" – כבר מדברים על דור רביעי מתישהו לקראת 2015. דור רביעי יאפשר גליש ה במהירות גבוהה יותר, נדידה בין רשתות wireless, רשתות לווייניות, ושאר אלחוטיות למיניהן. התשתית כבר אמורה להיות מתוכננת לתמוך בכל תקשורות המולטימדיה מבוססות IP הנפוצות כיום (קול, וידאו, דוא"ל, גלישה, messaging וכו') .

איך זה עובד?

ניקח לדוגמא רשת GSM:



רשימת רכיבים שמשתתפים בתהליך:

1. קליינט- יכול להיות טלפון סלולארי, מחשב נייד, PDA, או כל מכשיר אחר שתומך בדור שלישי.
2. Base station System (המלבן השמאלי) – רכיב רדיו המקבל ושולח אותות תקשורת אוויריים אל מול ההתקן.
   - Base Station Controller (BSC) - בעצם ה-"מוח" שאחראי על הקצאת המשאבים , ניתוב השיחות ועוד. הוא משמש בתור רכז לציודי קצה, ויכול לנהל מאות ציודים כאלה.
3. Network Switching Subsystem - הצד שאחראי על ניהול השיחות והעברת המידע- מהצד של הספקית שלנו. המערכת אחראית על מיתוג השיחות, והעברת השיחות החיצוניות הלאה אל ה-PSTN (רשת הטלפוניה הציבורית), ואף למרכזיות אחרות. הרבה מאוד פעמים המערכת מורכבת משירותי מיתוג לשירותים נוספים כגון WAP, SMS, MMS ואותיות אחרות באנגלית.
   - Mobile Switching Center (MSC)- הרכיב שאחראי על ניתוב השיחות, SMS, פקסים, שיחות ועידה וכו'. הרכיב אחראי על יצירתו וניתוקו של החיבור מקצה לקצה, חיובי השיחות, וניטור החשבונות.
   - HLR- מסד נתונים המכיל בתוכו את פרטי המשתמשים המורשים להשתמש ברשת ה- GSM המדוברת. מסד הנתונים מחזיק את כלל הנתונים עבור כל אחד מבעלי ה-SIM באותה רשת נתונה, ואת השירותים בהם כל אחד מהם מורשה להשתמש.

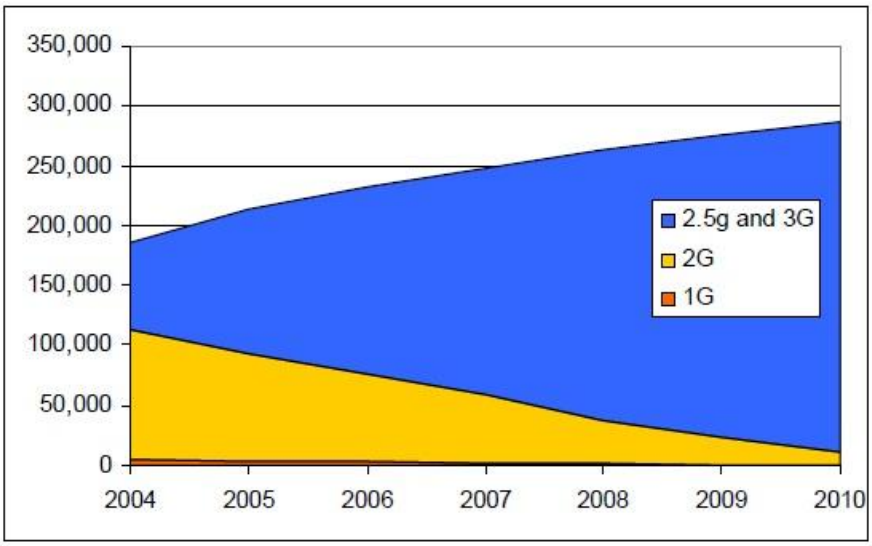
- VLR – מסד נתונים זמני אשר מכיל את פרטי המשתמשים ש"נדדו" לתוך הרשת. לכל רשת שכזו יש שרת VLR אחד, ולכן משתמש יכול להופיע רק ברשימת VLR אחד בכל רגע נתון.
- ישנם שירותים נוספים שיכולים להופיע כגון שירותי ציוד, שירותי תוכן, שירותי רדיוס וכד'.

הכל פה ממש על קצה המזלג, רק כדי להסביר מושגי יסוד ולתת ידע בסיסי. אם אתם רוצים להעמיק, כל אחד מהרכיבים הללו הוא עולם ומלואו. אני ממליץ על Google כמנוע חיפוש...

סיכונים קיימים:

מה שניסיתי להעביר עד עכשיו זה רעיון מאוד פשוט - חברות הסלולר מקבלות תפקיד חדש בחיים . אם עד היום הן היו ספקיות Voice, שזה נחמד, היום הן כבר הופכות להיות ממש ISP עם כל הכיף והאחריות שנלוות לכך. משמע, צריך להתחיל להשקיע ולתכנן צדדים רבים נוספים, והצד שמעניין אותנו הוא כמובן אבטחת מידע.

אפשר לראות לפי הגרף הבא את הגידול המשמעותי בצרכני הדור השלישי בעולם בשנים האחרונות:



Source: *iGR*, 2006

(במקור: http://www.iGR-inc.com)

להלן כמה מהבעיות שה ISP החדשות יצטרכו להתמודד מולם:

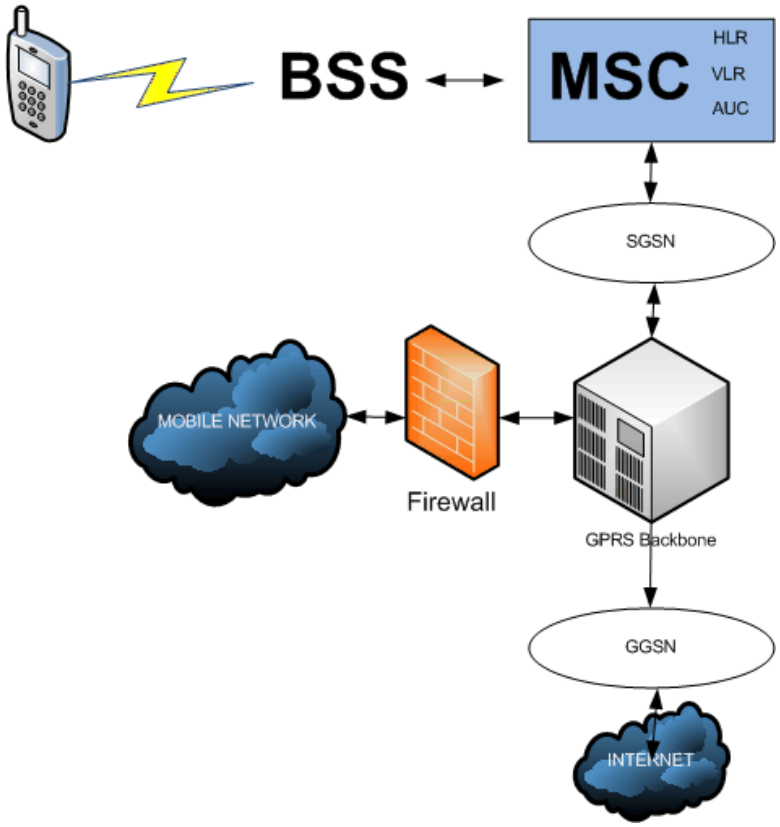
1. מכיוון שספקיות הסלולר עובדות מול תשתיות רדיו , ותשתיות מועטות רוחב פס , הן הרבה יותר פגיעות להתקפות Denial of Service. בתחילת הדרך היו מספר סיפורים על מחשב יחיד ששלח מספיק הודעות SMS בכדי להפיל את השרת שמספק את השירות.
2. תפוצת הוירוסים ושאר מזיקים למיניהם שמיועדים לטלפונים סלולאריים הולכת ותופסת תאוצה , בייחוד כאשר הוירוסים האלה יכולים להתפשט בדרכים נוספות כגון חיבורי Blue-Tooth לדוגמא. בנוסף היום קיימים צינורות כגון MMS שיודעים לעבור בין מייל לטלפון וחזרה.

3. SPAM, דואר זבל, ופרסום מסיבי, שהיו נחלתם של הדואר האלקטרוני בכמויות בלתי נתפסות, הולכים ומתקרבים אל המשתמשים גם במכשירים הסלולאריים.

מה שעוד "מקל" על מתקפות מהסוג הזה הוא שספקיות הסלולאר הן חדשות יחסית בתחום טכנולוגיות ה-IP, ולא בהכרח שמות את הדגש ההכרחי על ענייני אבטחת מידע.

רשתות הדור השלישי מציגות לנו הרבה חוליות חלשות בארכיטקטורה שלהם:

- **מכשיר הקצה** - הטלפון עצמו אמנם מפותח מאוד טכנולוגית אך אפליקציות הנוגעות לאבטחת מידע לוקות בחסר. בנוסף לכך, היות והמכשיר מחובר לאינטרנט, לדוא"ל, MMS, הוא פגיע למזיקים הרבים הקיימים ברשת.
- **הקישור האלחוטי בין המכשיר לבין רכיב ה- BS-Base Station** (ברוב המקרים מדובר באנטנות הסלולאריות) - הקישור מאובטח ברמת אבטחה גבוהה יחסית, וכולל פרוטוקולים חזקים של אימות והצפנה, מה שמקשה מאוד על האזנה לתעבורה. קיימת רגישות לתקיפות DATA מכיוון האינטרנט, ורשתות מידע חיצונית.
- **הקישוריות של הרשת הסלולארית מול ספקיות סלולאריות אחרות או מול רשתות מידע אחרות –** האינטרנט למשל. הקישוריות מול ספקיות אחרות מתבצעת בתצורה הבאה:



כאשר מכשיר סלולארי מתחבר לשירותי הדור השלישי הוא מתחבר אל ה-SGSN – Serving GPRS Support Node. ה-SGSN מתחבר בפרוטוקול GTP (GPRS Tunneling Protocol) אל מול ה-GGSN. ה-GGSN, הוא האלמנט ברשת שאחראי על תקשורת אל מולם העולם החיצוני.

פרוטוקול ה- GTP שנמצא בשימוש פה, מכיל פרטים לגבי מספר הטלפון והמנוי שיוצרים את הקשר, אך הפרוטוקול לא מכיל שום מנגנוני אימות נתונים , זיהוי, או הצפנה – מה שאומר שתוקף יכול "לחגוג" פה. הפרוטוקול נמצא בשימוש גם בין ה- SGSN לבין ה-GGSN, גם בין ה-GGSN לספקיות האחרות, ולבסוף, גם בין ה-GGSN לאינטרנט.

- **הקישור לשרתי הספקית עצמה (HLR, שרתי תוכן וכד')** – אפשר לנצל באגים ופגיעויות בפרוטוקולים הנמצאים בשימוש הספקית עצמה. למשל בפרוטוקול SIP, המשמש לתעבורת Voice Over IP – VoIP (טלפוניה). הפרוטוקול ידוע כפרוטוקול הרגיש להתקפות Buffer Overflow.

דרכי התמודדות:

ראינו שלא חסרות פגיעויות בארכיטקטורה ובמערכות הדור השלישי. מה ניתן לעשות בכדי להתמודד?

1. השלב הראשון, כמו תמיד, הוא התודעה. המשתמשים להפנים שהטלפונים נהיו חלק בלתי נפרד מרשת האינטרנט, והוא פגיע לכל הסכנות שמרוצצות להן שם בחוץ. ספקיות הסלולר חייבות להבין שהם ISP, ולדאוג לסידורי אבטחת המידע בהתאם.
2. הגנה מפני מזיקים- שמעתי פעם השוואה שטוענת שלחבר את המחשב הנייד לאינטרנט כאשר הוא לא מוגן באנטי-וירוס כזה או אחר זה בדיוק כמו ללכת לנערת ליווי בתאילנד מבלי להשתמש באמצעי מניעה. אותו הגיון צריך להיות מ ושרש גם במכשירי דור שלישי . כל מכשיר שמתחבר לאינטרנט צריך להיות עם הגנה מפני מזיקים ו-Firewall מקומי. בנוסף, גם לספקיות יש אחריות לבצע סריקות על השרתים שלהם ולהסיר את התולעים, רוגלות, ושאר תופינים שיימצאו שם.
3. Firewall – ספקיות הסלולר חייבות להטמיע הגנה על הרשתות שלהם בכל הרמות:
   - **Packet**- בדיקה האם כל חבילת מידע מורשה להיכנס לרשת על-פי הנתונים ב-Header של אותה חבילת מידע.
   - **Session**- בדיקה של זרימת חבילות המידע בין הרשתות, ובדיקה שכל חבילת מידע היא חלק מ-Session. קרי: "statefull inspection", גאווה לאומית.
   - **Application**- בדיקת תקינות חבילות המידע אל מול הגדרות הפרוטוקול בוא היא מדברת ב-L7, ובנוסף בדיקות חתימות אל מול מתקפות ידועות בעולם.

ישנם היום מוצרי Firewall שמיועדים במיוחד לרשתות דור שלישי שיודעים להתמודד עם סוגי התעבורה החדשים. בנוסף חשוב לציין כאן את החשיבות ביישום IDP ברשתות בסדר גודל הזה, בכדי לצמצם סיכויי התקפת DoS, על ציודי התקשורת.

4. VPN – דיברנו רבות (יחסית) על הפרוטוקול GTP ועל הפגיעויות הרבות הקיימות בו. על רבות מהבעיות שדיברנו אפשר להתגבר באמצעות הצפנת התעבורה ע"י IPSec VPN. בנוסף, היות ה-GGSN נקודת תקשורת אל מול גורמים חיצוניים, רצוי להשקיע, ו"למגן" אותו כמו שצריך.

מה לוקחים הביתה מכל זה?

ננסה לסגור את כל הקצוות. העולם מתקדם, הטכנולוגיה מתקדמת, אנחנו מנסים לעמוד בקצב – עד כאן שום דבר חדש. הטלפונים הסלולאריים הם היעד למתקפות העתיד, והאחריות שלנו היא לנהוג באחריות, לא להקל ראש, ולדאוג בראשונה לאבטחת המידע האישי שלנו. הרשתות הסלולאריות, למרות שמעניין מאוד ללמוד איך הן עובדות, הן לא באחריותנו, ולכן אנו - בתור משתמשים- נדאג למכשיר הקצה שלנו ולא להתקנת ציודים מורכבים בצמתי התקשורת

מבחינת השימוש במכשיר לצרכים ה נוגעים במידע מסווג – כבר היום יש אפליקציות המשמשות להצפנת המכשיר הנייד למקרה שייגנב או שיאבד.

לגבי קריאת מיילים ועבודה מול העבודה – בהנחה שבמשרד שלכם יישמו את הגישה למיילים בצורה מאובטחת, אין צורך להיגרר לפרנויות ולפחד מהאלחוט. הפרוטוקולים עצמם מספיק מאובטחים כדי שנוכל להשתמש בהם.

כמו בכל שיח על אבטחת מידע, העצה הכי טובה היא להשתמש בראש ולהפעיל שיקול דעת

והכי חשוב לא לשכוח שהסכנה הגדולה ביותר בטלפונים ניידים היא העובדה שהם מסרטנים.