

Digital Whisper

גליון 35, ספטמבר 2012

מערכת המגזין:

מייסדים:	אפיק קסטיאל, ניר אדר
מוביל הפרוייקט:	אפיק קסטיאל
עורכים:	שילה ספרה מלר, ניר אדר, אפיק קסטיאל,
כתבים:	סשה גולדשטיין, ישראל חורז'בסקי, אמיתי דן, עו"ד יהונתן קלינגר

יש לראות בכל האמור במגזין Digital Whisper מידע כללי בלבד. כל פעולה שנעשית על פי המידע והפרטים האמורים במגזין Digital Whisper הינה על אחריות הקורא בלבד. בשום מקרה בעלי Digital Whisper /או הכותבים השונים אינם אחראים בשום צורה ואופן לתוצאות השימוש במידע המובא במגזין. עשיית שימוש במידע המובא במגזין הינה על אחריותו של הקורא בלבד.

פניות, תגובות, כתבות וכל הערה אחרת - נא לשלוח אל editor@digitalwhisper.co.il

דבר העורכים

ברוכים הבאים לגליון ה-35 של Digital Whisper!

חודש אוגוסט עבר, וחודש ספטמבר בפתח, ואיתו הגליון החדש, הגליון ה-35! שלמרות כל כך הרבה לחץ החודש - הספקנו לעמוד בזמנים... החודש, אין לי יותר מדי דברי חוכמה להגיד, אז רק אעדכן אתכם בשני דברים שחודשו במגזין. הראשון הוא שינוי פני [עמוד הגליונות](#), לאחר כל כך הרבה בקשות, פניות במייל ותגובות באתר מצאנו קצת זמן פנוי וסידרנו את העמוד, כך שעכשיו ניתן לחפש ביתר קלות מאמר ספציפי על פני כל הגליונות שפורסמו עד כה. מדובר בגרסא יחסית זמנית של העמוד, אני מקווה שבעתיד הקרוב נוסיף חיפוש לפי תגיות על מנת להקל באיתור מאמר ספציפי או מאמר מנושא ספציפי. תרגישו חופשי לתת הערות.

הדבר השני הוא שינוי פני הגליונות הקודמים ויישור קו עם העיצוב הנוכחי. אני לא יודע אם אתם זוכרים איך הגליון הראשון היה נראה, אבל תרשו לי לחוות דעה: הוא היה נראה נורא, (שלא נאמר... זוועה... ©), מבחינת תבנית כמעט אין הבדל, אך מבחינת עימוד, מרווח בין שורות, לוגו ושאר דברים קטנים שעושים את הטקסט יותר נעים בעין שינוי הכל - לדעתי ההבדל הוא עצום. אז לקחתי על עצמי לערוך את הגליונות הישנים ולעדכן אותם עם התבנית הנוכחית. נכון לעכשיו אני בגליון הרביעי, אך לאט לאט אני אעבור על כולם (מבדיקה שלי, בסביבות הגליון ה-17 עברנו לעיצוב הנוכחי פחות או יותר).

בנוסף,

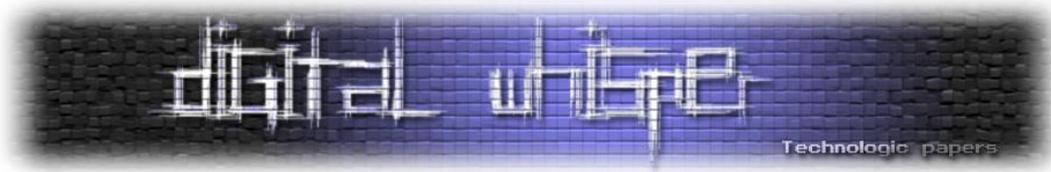
הייתי רוצה לנצל במה זו, לאחל לאישתי מזל טוב לרגל שנתיים (ויום) של נישואין. **לא יכולתי לבקש אישה מדהימה יותר, מבינה יותר ותומכת יותר.** קוראים יקרים, אתם חייבים לה הרבה... ☺

זוהו פחות או יותר, אם יש לכם רעיונות נוספים לשיפור המגזין - נשמח לשמוע עליהם!

כמובן, לפני הכל, רצינו להגיד תודה לכל מי שישב, והקדיש לכם מזמנו הפנוי וכתב לנו מאמרים: תודה רה **לסשה גולדשטיין!** תודה רבה **לישראל חורז'בסקי!**, תודה **לאמיתי דן!** ותודה רבה **לעו"ד יהונתן קלינגר!** בלעדיכם לא היינו פה החודש ☺

שתהיה קריאה נעימה!

אפיק קסטיאל וניר אדר.



תוכן עניינים

2	דבר העורכים
3	תוכן עניינים
4	איסוף זבל ב-.NET
12	חולשות ב-SSL
31	זיהוי אנשים ומטופלים על פי מבנה כף יד ורנטגן
41	אינטרנט לא חברותי
46	דברי סיום

איסוף זבל ב-.NET

נכתב ע"י סשה גולדשטיין

הקדמה

בהמשך למאמר בגיליון חודש יוני, אנו מתקדמים בסקירתנו את המימוש הפנימי של .NET. ובמאמר זה נבחן את פעולתו של אוסף הזבל (garbage collector) ומבנה הערימה המנוהלת (GC heap) שעליה הוא פועל. כידוע, איסוף הזבל הוא המאפיין המרכזי של סביבות מנוהלות כגון Java ו-.NET. ומקל משמעותית על המתכנת כיוון שכעת ביכולתו להתעלם מהצורך בשחרור מפורש של אובייקטים מהזיכרון.

לאוסף הזבל חשיבות מכרעת לביצועים גבוהים ביישומי צד שרת, משחקים רגישים לעיכוב, מערכות זמן אמת ועוד רבות אחרות. לכן אופן פעולתו מורכב יחסית, כדי לאפשר ביצועים גבוהים לסוגים שונים של תוכניות. אם התקורה של אוסף הזבל עולה על התקורה של ניהול ידני של זיכרון, זה עשוי להיות לא משתלם חרף הרווח הגדול ביעילות הפיתוח.

נתחיל בסקירה כללית של פעולת אוסף הזבל בשיטת סימון ומחיקה (mark and sweep) ולאחר מכן נכנס לפרטים. עוד לפני שנתחיל יש צורך לציין שאוסף הזבל של .NET אינו פועל בשיטת מניית התייחסויות (reference counting), שאינה מקובלת באופן כללי באוספי זבל של שפות עילית מודרניות. תוכלו לקרוא עוד על [מניית התייחסויות בוויקיפדיה](#) וכן לעיין בפרטים אודות [אוסף הזבל של Python](#), המשתמש בין היתר במניית התייחסויות.

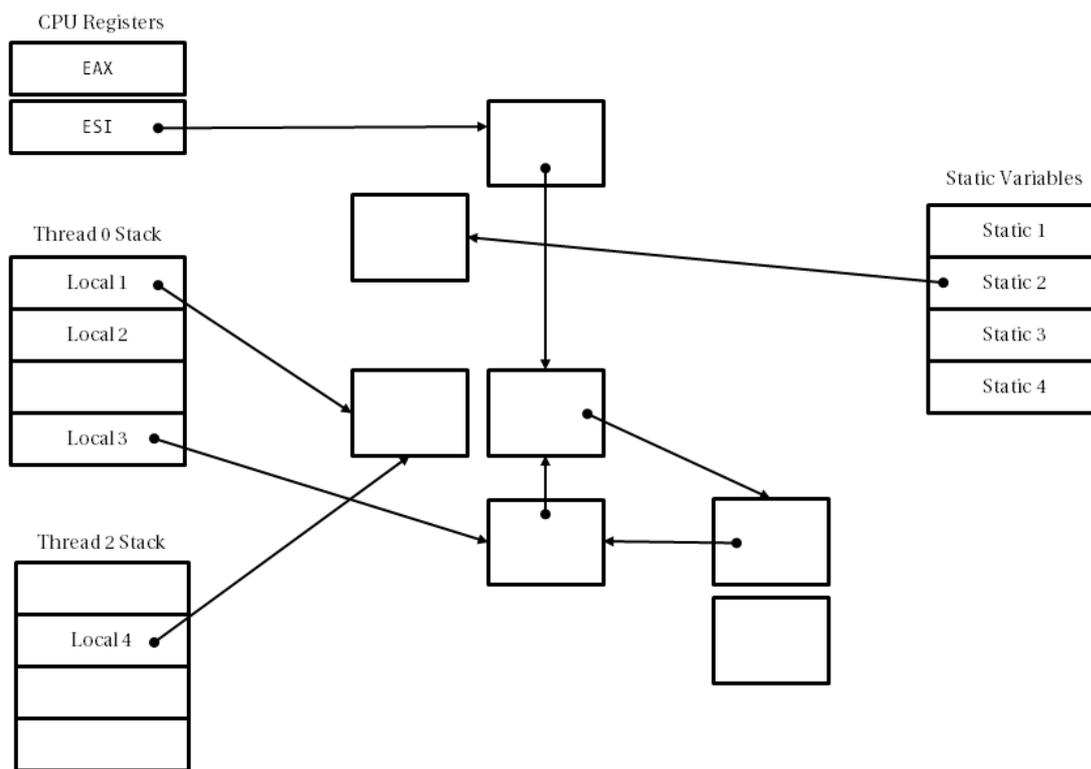
סימון ומחיקה

העיקרון הבסיסי העומד ביסוד פעולתו של אוסף הזבל הוא מושג הישיגות (reachability). אוסף הזבל נדרש להשאיר בערימה את האובייקטים הישיגים, אלה שהתוכנית עשויה להשתמש בהם בהמשך, ולמחוק מן הערימה את שאר האובייקטים (הזבל). ההגדרה של ישיגות היא רקורסיבית, ונובעת מהאופן שבו תכניות יכולות לגשת לאובייקטים באופן כללי:

1. אובייקט הוא ישיג אם יש מצביע אליו ממשתנה סטטי של מחלקה טעונה כלשהי.
2. אובייקט הוא ישיג אם יש מצביע אליו ממשתנה מקומי של שיטה המתבצעת כרגע.
3. אובייקט הוא ישיג אם יש מצביע אליו מאוגר (register) של מעבד כלשהו המבצע את התוכנית.
4. אובייקט הוא ישיג אם יש מצביע אליו מאובייקט ישיג.

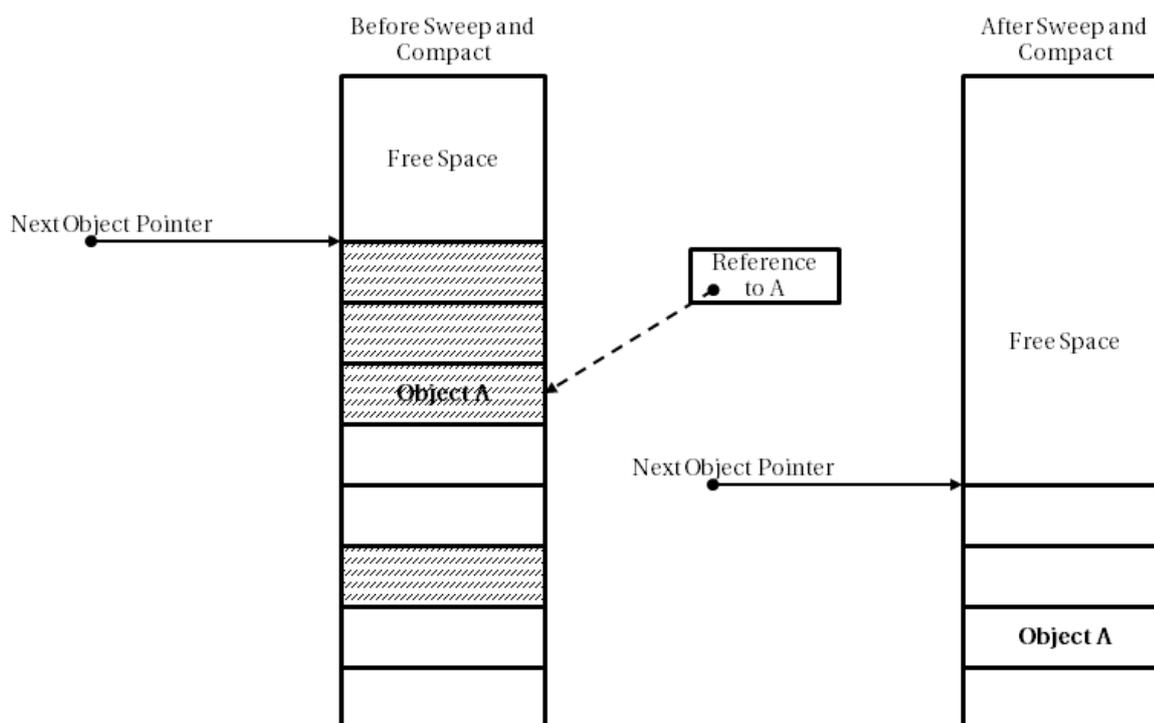
יש לשים לב שהגדרת ישיגות זו רחבה יותר מאשר "האובייקטים שהתוכנית משתמשת בהם". יתכן שמשנתה סטטי מסוים מכיל מצביע לאובייקט שלא יעשה בו שימוש עד סוף ריצת התוכנית. עם זאת, אוסף הזבל לא יכול לקבוע האם התוכנית תעשה שימוש במצביע מסוים (הדבר שקול לבעיית העצירה, שאינה כריעה על ידי מחשב), ולכן הגדרת ישיגות זו היא האופן שבו פועלים כל אוספי הזבל בשיטת סימון ומחיקה.

אם כן, כדי למצוא את האובייקטים המיועדים למחיקה (הזבל), על אוסף הזבל למצוא תחילה את האובייקטים הישיגים. הדבר מתבצע על ידי חיפוש רגיל בגרף, תוך סימון האובייקטים הישיגים ב-object header word שהוזכר במאמר הקודם. נקודות ההתחלה של החיפוש הם המשתנים הסטטיים של כל המחלקות הטעונות, והמחסניות של החוטים הפעילים שבהן נמצאים המשתנים המקומיים של שיטות המתבצעות כרגע. בניגוד לאוספי זבל מסוימים אחרים, אוסף הזבל של .NET הוא מדויק ביחס למשתנים מקומיים: יש ברשותו תמיד מידע עדכני על המשתנים המקומיים של כל שיטה, ולא ניתן להכשילו על ידי משתנים שאינם מכילים מצביעים אך שנראים כמו כאלה (למשל, float שערך הביטים שלו נראה כמו מצביע לתוך הערימה).



בסוף שלב הסימון אוסף הזבל פונה למחיקת האובייקטים הלא-ישיגים. על מנת לשמור על רציפות הזיכרון ולקבל ביצועים טובים יותר בזמן הקצאת אובייקטים, אוסף הזבל של .NET מבצע מעת לעת דפרגמנטציה של הערימה, על ידי דחיסת האובייקטים הישיגים למקטע זיכרון רצוף (מה שכתוב בהזזה של אובייקטים ישיגים ועדכון המצביעים אליהם כדי שימצאו אותם במקומם החדש). לאחר פעולה זו, ניתן לחלק את

הערימה למקטע שמכיל אך ורק אובייקטים ישיגים ומקטע שהוא פנוי לחלוטין, וכך עלות ההקצאה מהערימה היא אפסית כמעט וכרוכה רק בקידום מצביע המכונה next object pointer, בדיוק כמו הקצאת זיכרון מהמחסנית באמצעות ה-stack pointer.



עצירת חוטים

כאשר אוסף הזבל מתחיל במעבר על הערימה המנוהלת, נשאלת השאלה: האם שינויים המתבצעים ע"י חוטים אחרים בתוכנית ועלולים להביא לתוצאות איסוף לא מדויקות? נראה שכך המצב, ונדמה שאין ברירה אלא לעצור את כל החוטים של התוכנית בכל מהלך פעולתו של אוסף הזבל. לגישה זו, המכונה stop-the-world, חיסרון עצום: בפועל על ערימה גדולה (של מספר ג"ב), אוסף הזבל עשוי לעצור את כל התקדמות התוכנית למספר שניות ואף דקות! יתר על כן: עצירה של חוטים אחרים בצורה אכזרית (SuspendThread דומיו) מסוכנת מאוד, ובפועל אוספי זבל נוקטים בשיטה המבוססת על שיתוף פעולה בין חוטי התוכנית לבין החוט של אוסף הזבל. שיתוף פעולה זה יקר מאוד ומכניס עיכובים נוספים (עד מאות מ"ש) הדרושים רק לשם עצירת החוטים בהכנה לתהליך האיסוף.

אלא שכבר מגרסתו הראשונה, אוסף הזבל של .NET. מאפשר עצירה חלקית של החוטים האחרים בתוכנית. למעשה, אוסף הזבל מאפשר בחירה באיסוף בו-זמני (concurrent), הדורש עצירה של החוטים האחרים

בעיקר במהלך שלב המחקר אך לא בשלב הסימון. אובייקטים חדשים המתווספים לערימה במהלך הסימון ושינויי מצביעים לאובייקטים במהלך שלב הסימון דורשים התייחסות מיוחדת של אוסף הזבל, כדי שלא לפנות אובייקטים הנמצאים עדיין בשימוש התוכנית.

בגרסאות האחרונות של .NET, אוסף הזבל השתכלל בהרבה בכל הקשור לביצוע איסוף במקביל לפעולת התוכנית. ראשית, כברירת מחדל אוסף הזבל פועל היום בתצורה בו-זמנית הן בצד השרת והן בתחנות עבודה. אוסף הזבל מפעיל מספר חוטים הרצים ברקע ומבצעים איסוף זבל כמעט ללא עצירה של חוטי התוכנית, והאוספים את הזבל במקביל תוך ניצול ריבוי הליבות (או המעבדים) הקיים היום כמעט בכל מחשב. על אף שאוסף הזבל של .NET. עדיין נמצא מאחור ביחס למוצרים כגון Azul Pauseless GC עבור JVM, כבר היום משך עצירת החוטים והתקורה הנגרמת מאיסוף זבל המתרחש לעתים קרובות הצטמצמו משמעותית ומספקים את הדרישות אפילו של מערכות זמן אמת מסוימות (למערכות רגישות באמת .NET. מאפשרת גם לבקש לצמצם את פעולת אוסף הזבל באמצעות API מפורש המכונה GC.LatencyMode).

דורות

אחת הסיבות לעצירות ממושכות של המערכת בזמן איסוף הזבל היא הצורך לעבור על כמות גדולה של אובייקטים בזיכרון. בתוכנית המשתמשת באופן קבוע ב-1 ג"ב של זיכרון ומקצה לעתים רחוקות אובייקטים חדשים, כל סיבוב איסוף זבל מחייב סימון של כל האובייקטים הישיגים בערימה. אפילו אם כל האובייקטים אכן נמצאים בזיכרון הפיזי זוהי פעולה ממושכת יחסית (מאות מ"ש), ואם מקצת מהאובייקטים דופדפו לקובץ ההחלפה (pagefile), זמן זה יכול להאמיר לשניות ארוכות. כדי לצמצם עלויות אלה, אוסף הזבל מבחין בין אובייקטים חדשים לאובייקטים ותיקים, ומנצל שתי תכונות ניסיוניות שבדרך כלל מתבררות כנכונות לגבי רוב התוכניות:

1. אובייקטים חדשים מתים מהר.

2. אובייקטים ותיקים נוטים להישאר בחיים זמן ממושך.

תכונות דומות ידועות בתחום מערכות ההפעלה לגבי זמני ריצה של תהליכים - תהליכים שרצו כבר זמן

על שמירת סיסמאות בזיכרון

בדומה לדפים המוקצים ישירות בעזרת VirtualAlloc שמגיעים לתוכנית מלאי אפסים (zero pages), אובייקטים או חוצצים המוקצים ב-.NET. נדרסים באפסים לפני שהתוכנית יכולה לעשות בהם שימוש. אלא שלא יסוף הזבל חיסרון מסוים, כיוון שאין לדעת מתי הזיכרון שאינו נמצא בשימוש יוחזר למערכת ההפעלה או ינוקה מתוכן. בהחלט ייתכן שמידע רגיש שנשמר בחוצץ או מחרוזת בזיכרון לא יימחק ולא יידרס באפסים במשך שעות ארוכות.

על מנת להתמודד חלקית עם אתגר זה, .NET מספקת מחלקה הנקראת SecureString המבטיחה שתווי המחרוזת נשמרים בזיכרון בצורה מוצפנת בלבד. הדבר אינו מונע חשיפה של המידע כיוון שגם מפתח ההצפנה נמצא בזיכרון, וישנם גם API-ים מפורשים להמרה של SecureString למחרוזת רגילה (כגון Marshal.SecureStringToBSTR), אך מדובר בהגנה ראשונית בפני דליפת מידע לא מכוונת במסגרת התוכנית. דוגמא לשימוש:

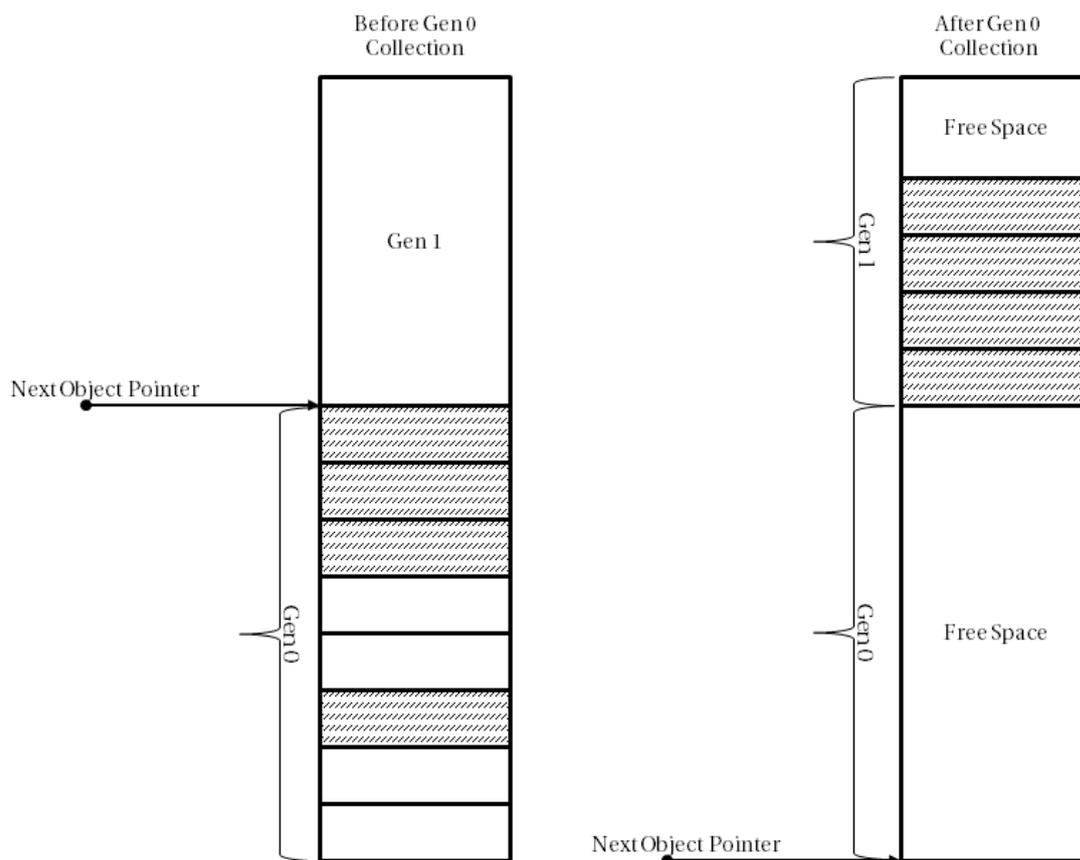
```
ConsoleKeyInfo key;  
var pwd = new SecureString();  
while(true) {  
    key = Console.ReadKey(true);  
    if (key.Key ==  
        ConsoleKey.Enter) break;  
    pwd.AppendChar(key.KeyChar);  
}  
Process.Start("calc.exe",  
    "Administrator", pwd, null);
```

ממושך צפויים להמשיך לרוץ עוד זמן רב, בעוד שתהליכים שנוצרו זה עתה צפויים להסתיים בקרוב. בתחום מערכות ההפעלה נעשה שימוש בתכונות אלה על מנת לבצע תזמון חכם של תהליכים; בתחום איסוף הזבל לתכונות אלה חשיבות מכרעת בחלוקת הערימה לאזורי איסוף נפרדים (דורות).

אוסף הזבל של .NET מחלק את הערימה לשלושה דורות (generations) - דור 0 לאובייקטים חדשים לגמרי, דור 1 לאובייקטים פחות חדשים, ודור 2 לאובייקטים ותיקים. המעבר בין הדורות מתרחש כאשר מתבצע איסוף זבל - אובייקט בדור 0 ששרד סיבוב איסוף אחד יעבור לדור 1, אובייקט בדור 1 ששרד דור איסוף נוסף יעבור לדור 2. אלא שבבואו לבצע איסוף זבל, אוסף הזבל לא מסמן את כל האובייקטים הנמצאים בערימה, אלא רק את האובייקטים בדור המיועד לאיסוף (condemned generation) והדורות שמתחתיו.

כך למשל, כאשר נגמר המקום בדור 0 (שגודלו מצומצם מאוד ויכול להיות מספר מ"ב בודדים) אוסף הזבל יבצע סבב סימון ומחיקה בדור 0 בלבד. זוהי פעולה זולה מאוד מאחר שדור 0 בדרך כלל נכנס בזיכרון המטמון של המעבד, וממילא מדובר על כמות קטנה יחסית של אובייקטים שיש לסמן. האובייקטים השורדים

יעברו לדור 1 ופעולת האיסוף תסתיים במהרה. באופן דומה, כאשר נגמר המקום בדור 1, מתבצע איסוף זבל בדור 1 - וכדומה.



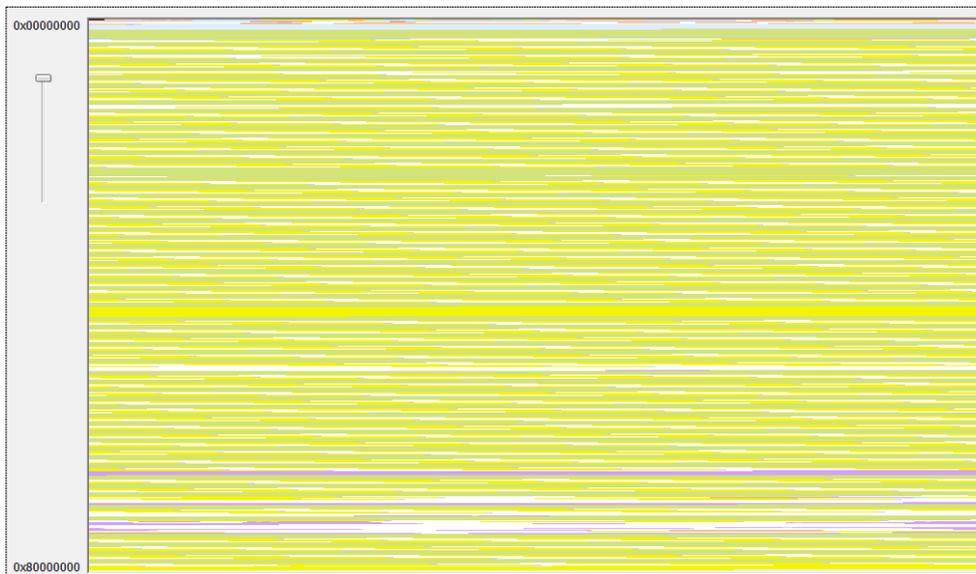
התועלת הגדולה משיטת האיסוף הדורות עולה מהתבוננות בהנחות (1) ו-(2) שצוינו מעלה. כאשר אוסף הזבל מסמן ומנקה את דור 0, רבים הסיכויים שרוב האובייקטים בדור 0 אינם ישיגים ולכן ניתנים לפינוי. כלומר, למרות שדור 0 קטן ויתרחשו בו סבבים תכופים של איסוף זבל, אלה יהיו סבבים יעילים ומהירים כיוון שרוב האובייקטים ניתנים למחיקה ולא דורשים עבודה נוספת מצד אוסף הזבל.

המשמעות העיקרית עבור תכניות היא החשיבות בשמירה על הנחות (1) ו-(2) לעיל. כלומר, על תכניות מנוהלות לבצע הקצאות ארוכות טווח בתחילת הריצה ולא לשחרר לעתים קרובות אובייקטים ותיקים, ומאידך לדאוג לשחרור מהיר ככל האפשר של אובייקטים חדשים (זמניים) כדי שיוכלו להיאר עוד בדור 0. מניסיון רב שנים בתחום עולה שתוכניות הפועלות לפי הנחיות אלה משיגות שיפור של מספר סדרי גודל בזמני איסוף הזבל, ומגיעות למצב בו איסוף הזבל כמעט ואינו מורגש ברקע ריצת התוכנית.

הקצאת זיכרון ממערכת ההפעלה

מהדיון קודם בניהול הערימה ע"י אוסף הזבל מתבהר שלעיתים קרובות מקטעים רחבים של הערימה פנויים מאובייקטים לחלוטין. עם זאת, אוסף הזבל לא מחזיר אותם מיידית למערכת ההפעלה, ולמעשה אוסף הזבל גם לא פונה למערכת ההפעלה עבור כל הקצאה של אובייקט חדש - משיקולי ביצועים. אוסף הזבל אף אינו משתמש במנגנוני ניהול הערימה של חלונות, כגון HeapAlloc/HeapFree, אלא פונה ישירות למנהל הזיכרון הווירטואלי באמצעות VirtualAlloc.

אוסף הזבל מבקש ממערכת ההפעלה מקטעי זיכרון גדולים המכונים סגמנטים, שגודלם נע בין 64-16 מ"ב רצופים במערכות 32 ביט ועד מספר ג"ב רצופים במערכות 64 ביט. מדובר בשיריון כתובות בלבד, שמתהווה להקצאה של זיכרון ממש רק כאשר נעשה בדפי הזיכרון שימוש.



על ידי בקשה של מקטעי זיכרון גדולים, אוסף הזבל מצמצם את התקורה הכרוכה בפנייה לשירותים של מערכת ההפעלה (system calls) וכן בניהול טבלאות תרגום של כתובות וירטואליות לכתובות פיזיות (page tables). עם זאת, לשיטת הסגמנטים גם חיסרון משמעותי, בעיקר במערכות 32 ביט שבהן מרחב הכתובות מוגבל מאוד.

במערכת הפועלת שעות וימים ארוכים ומבצעת כמות משמעותית של הקצאות הן מהערימה המנוהלת והן ממקורות אחרים במערכת ההפעלה (כגון טעינה של DLL-ים או הקצאה של זיכרון מהערימה הלא-מנוהלת), עשויה להיווצר פרגמנטציה חמורה של מרחב הכתובות הווירטואליות, עד כדי כך שהקצאות לא תצלחנה למרות שקיימים עדיין דפים פנויים רבים. תופעה זו היא אחת הסיבות למנגנוני מחזור (recycling)

אוטומטיים המופעלים היום כמעט בכל יישום צד-שרת, והדואגים להפעיל את התהליך מחדש לאחר מספר שעות/ימים כדי לקבל מרחב כתובות "טרי" ללא פרגמנטציה. לאבחון של תופעות פרגמנטציה מסוג זה, היישום VMMMap מבית Sysinternals מועיל מאוד (ובאמצעותו נוצר האיור הקודם).

סיכום

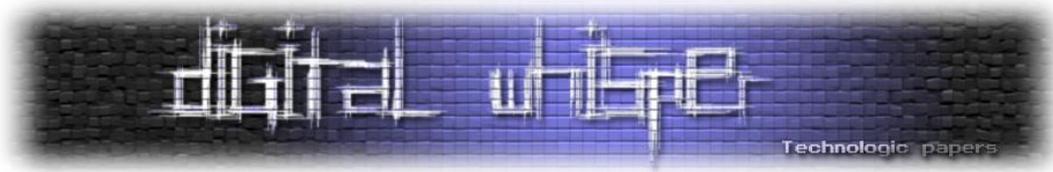
במאמר זה סקרנו את אופן פעולתו של אוסף הזבל ב-.NET, ונחשפנו מעט לשיקולים העומדים בבסיס מימושו הפנימי. למרות תחרות קשה מצד אוספי זבל מסחריים אחרים, והתקדמות מהירה בתחום גם מן המישור האקדמי, אוסף הזבל של .NET מצליח לענות על דרישותיהן של רוב היישומים המנוהלים ומצדיק את היתרון העצום ביעילות הפיתוח שמספקות השפות המנוהלות.

קצרה היריעה מכדי להיכנס לעומק בכל הקשור לאיסוף זבל ב-.NET, ולמעשה ראינו רק את קצה הקרחון. בספרי החדש [Pro .NET Performance](#) (הצפוי לצאת במהלך החודש הקרוב) יש כ-60 עמודים המוקדשים בלעדית לנושא איסוף הזבל (ממנו שאלתי גם את האיורים), וישנם גם מקורות נוספים באינטרנט שתוכלו להיעזר בהם להעמקה.

על המחבר

סשה גולדשטיין הוא ה-CTO של [קבוצת סלע](#), חברת ייעוץ, הדרכה ומיקור חוץ בינלאומית עם מטה בישראל. סשה אוהב לנבור בקרביים של Windows וה-CLR, ומתמחה בניפוי שגיאות ומערכות בעלות ביצועים גבוהים. סשה הוא מחבר הספר Pro .NET Performance, ובין היתר מלמד במכללת סלע קורסים בנושא Windows Internals-I Internals. בזמנו הפנוי, סשה כותב [בלוג](#) על נושאי פיתוח שונים.





חולשות ב-SSL

נכתב ע"י ישראל חורז'בסקי / Sro (AppSec Labs)

הקדמה

מאמר זה מיועד לכאלה ששמעו על המושג SSL, שמעו על המושג מפתח ציבורי, מפתח פרטי ומונחים דומים, ורוצים להכיר קצת ממגוון החולשות של SSL. במאמר זה ניגע בחולשות אלו בקצרה. לא יהיו פה אלגוריתמים, אותם ניתן להשיג בקלות בויקיפדיה. החלק הראשון נכתב באופן קצת סאטירי, אבל אל דאגה, בסיומו תצאו עם רשימת בעיות ב-SSL שאת חלקן מרבית האנשים לא מכירים. החלק השני כתוב בסגנון רציני יותר והוא מסכם בדיקות שביצעתי בשביל למצוא, נכון להיום, עד כמה החולשות מסוכנות.

קצת מונחים לפני הכל...

מי אתה מר SSL?

כינוי: SSL

ר.ת: Secure Socket Layer

שכבה: 6 במודל OSI

מה התפקיד שלך?

אני בא לפתור בעיית אבטחה.

מה הבעיה?

כאשר מתבצעת תקשורת בין מחשבים שונים על גבי הרשת (כמו למשל, בעת גלישה לאתר אינטרנט), ישנן שיטות רבות לחבל בתעבורה, ולגרום לה לעבור דרך מחשב שלישי - מחשב הנמצא ברשותו של התוקף. מתקפה זו שבה אנחנו מעבירים את התעבורה דרך מחשב הנמצא ברשותינו נקראת מתקפת Man In The Middle (או בקיצור "MITM").

תוכל למנות מספר דוגמאות למימוש MITM?

בהחלט! אמנה מספר שמות אך לא אכנס לעומק, במידה ותרצו, תוכלו לחפש עליהן בגוגל:

- **ARP Poisoning** - מתקפה אשר ניתן לבצע ברשתות LAN, במהלך המתקפה התוקף מרעיל את טבלת ה-ARP של הקורבן ושל הנתב, על מנת לגרום לכל אחד לחשוב שהוא השני. למידע נוסף:

http://en.wikipedia.org/wiki/ARP_spoofing

- **DNS Hijacking** - מתקפה אשר במסגרתה תוקף גורם לקורבן לחשוב כי כתובת IP של שרת הנמצא ברשותו הינה ה-Resolution של כתובת DNS מסויימת שאותה הקרבן מחפש. למידע נוסף:

http://en.wikipedia.org/wiki/DNS_hijacking

- **MAC flooding** - מתקפה אשר באמצעותה תוקף יכול לגרום למתג (Switch) לנתב אליו / לכלל הרשת מידע שהיה אמור להגיע לנמען (כתובת mac) ספציפי, למיע נוסף:

http://en.wikipedia.org/wiki/MAC_flooding

אוקי, אז המידע עובר דרך צד שלישי, מה הבעיה בזה?

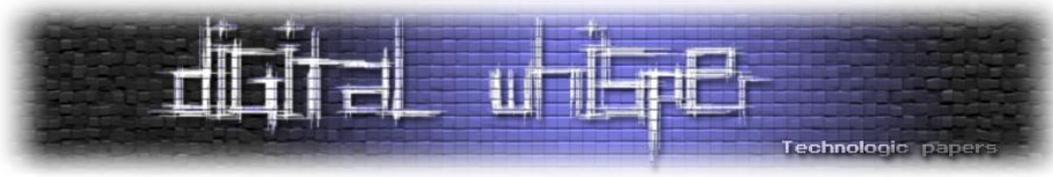
כאשר מידע עובר לנמען דרך צד שלישי, הצד השלישי יכול לבצע במידע כרצונו - הוא יוכל לחשוף את המידע, להשתמש בו לרעה, לפגום במידע, לשנותו ולפגוע באמינותו, למנוע את העברתו ליעד המקורי, ולבצע בו עוד פעולות רבות.

וואלה, בעיה. אז איך אתה מציע לפתור את הבעיה?

על מנת למנוע ממקרים כאלה להתרחש, אני מציע להגביר את רמת האמינות של תווך התקשורת. לדוגמא, ע"י זיהוי הגורמים בשיחה ואימות זהותם מול גורם אמין, על ידי בדיקה כי המידע אשר נשלח ממחשבו של צד אחד אכן הגיע לצד השני בשלמותו וללא שום שינוי. אני מציע להצפין את המידע הנשלח באופן כזה שרק הגורמים בשיחה יוכלו לפענח את המידע מבלי שגורם שלישי יוכל לעשות זאת.

אבל היי, בשביל להצפין צריך שגם למחשב שלי וגם לשרת שאליו אני פונה יהיה מפתח הצפנה זהה, לא?

כן ולא! וזה בדיוק הנושא הבא שלנו ☺



דיפי הלמן ושות'

שם: אחד מאיתנו Diffie השני Hellman.

מקצוע: מתמטיקאים

אז מה גילו דיפי-הלמן ששווה להזכיר אותם?

דיפי והלמן מצאו שיטה שבה כל אחד יכול לבחור מספר (להלן: מפתח פרטי) לבצע עליו חישובים מסוימים ולפרסם את התוצאה (להלן: מפתח ציבורי). נניח כי דיפי רוצה לכתוב משהו להלמן, הוא לוקח את המפתח הציבורי שהלמן פרסם, ואת המפתח הפרטי שלו עצמו, ומבצע חישוב מתמטי שכולל את שני המפתחות האלה. תוצאת החישוב תהיה מספר חדש (להלן: מפתח ההצפנה), עם המפתח הזה הוא מצפין את התעבורה, ושולח את התעבורה המוצפנת להלמן. הלמן שמקבל את התעבורה המוצפנת מדיפי, לוקח את המפתח הפרטי שלו (של הלמן) ואת המפתח הציבורי של דיפי ומבצע את אותו חישוב. המעניין בחישוב הוא, שניתן גם באמצעות חישוב של המפתח הפרטי של הלמן והמפתח הציבורי של דיפי, וגם באמצעות המפתח הפרטי של דיפי והמפתח הציבורי של הלמן, להגיע לאותו מספר.

כעת, כאשר יש להלמן את מפתח ההצפנה, בקלות הוא יכול לפענח את התעבורה המוצפנת.

נו, אז מה הבעיה?

הבעיה? השאלה היא איך דיפי יידע מה המפתח הציבורי של הלמן, ואיך הלמן יידע מה המפתח הציבורי של דיפי.

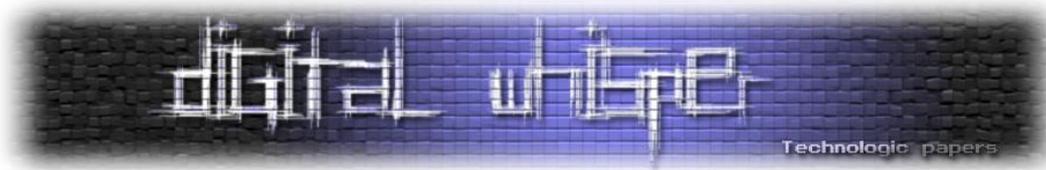
שישאלו אחד את השני...

זה אכן מה שעושים, אבל אם הפעולה הזו מתבצעת במרחב האינטרנטי, באמצעות מתקפת MITM הנ"ל, ניתן "לעבוד" על שניהם ולפענח את התעבורה.

מה זאת אומרת?

אז ככה, יש לנו את המחשב של **דיפי** שפונה לשרת של **הלמן** ויש את **התוקף** שמאזין באמצע. כאשר **דיפי** פונה ל**הלמן** על מנת לקבל ממנו את המפתח הציבורי שלו, **התוקף** עוצר את הבקשה בדרך, מייצר מפתח פרטי ומפתח ציבורי משל עצמו ואומר ל**דיפי** (בשם **הלמן**) כי זה המפתח הציבורי שלו - (של **הלמן**). **דיפי** מצפין את התעבורה עם מפתח ההצפנה שהוא יוצר באמצעות המפתח שלו יחד עם המפתח הציבורי של **התוקף** כשהוא חושב שזה המפתח הציבורי של **הלמן**.

בינתיים התוקף לא נח, פונה ל**הלמן** ומזדהה כ**דיפי**, ואומר לו: "זה המפתח הציבורי שלי, תעביר לי בבקשה את המפתח הציבורי שלך כדי שנוכל לתקשר בצורה מאובטחת". **הלמן**, בטוח שהוא מדבר עם **דיפי** ומביא לו את המפתח הציבורי שלו - של **הלמן**, ולוקח מה**תוקף** את המפתח הציבורי של **התוקף**.



בתור המפתח הציבורי של **דיפי**. **הלמן** לוקח את המפתח הפרטי שלו - של **הלמן** יחד עם הציבורי של **התוקף** ויוצר מפתח הצפנה.

כעת **דיפי** פונה ל**הלמן**, שולח תעבורה שמוצפנת למעשה עם מפתח ההצפנה **שלו** ושל **התוקף** (כל שילוב של אנשים יוצר מפתח שונה). **התוקף עוצר את התעבורה באמצע, מפענח אותה, קורא/משנה אותה, מצפין עם מפתח ההצפנה שהוא יצר עם הלמן ומעביר להלמן.**

ל**הלמן** אין אפשרות לדעת שיד התוקף בדבר, **והוא** יחזיר חזרה תעבורה ל**דיפי** דרך התוקף. **הוא** יצפין עם המפתח שהוא חושב שהוא של **דיפי**, התוקף יפענח ויצפין עם המפתח **שלו** עם **דיפי**.

כולם בטוחים שהכל בטוח, וזה בדיוק המתכון להתרסקות, Gave Over.

סיפור יפה, אבל... מישהו במרחב האינטרנטי מסכים להשתמש בשיטה הזו?

תתפלא, שרת WAMP תומך בהצפנה שכזו... היא נקראת ADH - Anonymous Diffie Hellman.

באמת?!

בעיקרון אל דאגה, אם הדפדפן שלך עדכני, הוא לא יסכים להתחבר בהצפנה הזו, ויגיד שיש בעיה עם ההצפנה.

יש אלגוריתמים נוספים?

אלגוריתם אחר שייך לשלישיית RSA, שלושה חוקרים שיצרו מנגנון שמזכיר את אלגוריתם החלפת המפתחות של דיפי-הלמן, אך יש בו שינוי מהותי. ההצפנה ב-RSA היא באמצעות המפתח הציבורי של הנמען נטו, בלי שום מפתח של השולח. כך שאם דיפי רוצה לשלוח משהו להלמן, הוא מצפין עם המפתח הציבורי של הלמן בלבד. דיפי יכול רק להצפין עם המפתח הציבורי של הלמן, הוא לא יכול לפענח חזרה את מה שהוא הצפין. רק הלמן שיש לו את המפתח הפרטי (שהמפתח הציבורי הוא תוצאה של חישוב שבוצע עליו) יכול לפענח את ההצפנה.

אז מה, מצפינים את כל התעבורה עם המפתח הציבורי? זה לא לוקח הרבה זמן?

לא, מצפינים רק את המפתח, את היתר מצפינים באמצעות מספר שיטות סימטריות אחרות - פעולה יותר פשוטה מבחינת משאבים.

סאטירי מה?

סימטרי. כל הצפנה נעשית באמצעות מפתח הצפנה. אם ניתן באמצעות אותו מפתח לפענח את ההצפנה (צפנים שכאלה הן המוכרות כמו א"ת-ב"ש, צופן קיסר וכן הלאה) הוא נקרא צופן סימטרי מכיוון שמפתח ההצפנה זהה למפתח הפענוח. אם באמצעות מפתח ההצפנה לא ניתן לפענח את ההצפנה (וזוה מה שייחודי בצופן RSA) הוא נקרא א-סימטרי (א = לא), בצופן א-סימטרי חוץ ממפתח ההצפנה קיים מפתח שמשמש לפענוח המידע המוצפן.

חולשות ב-SSL

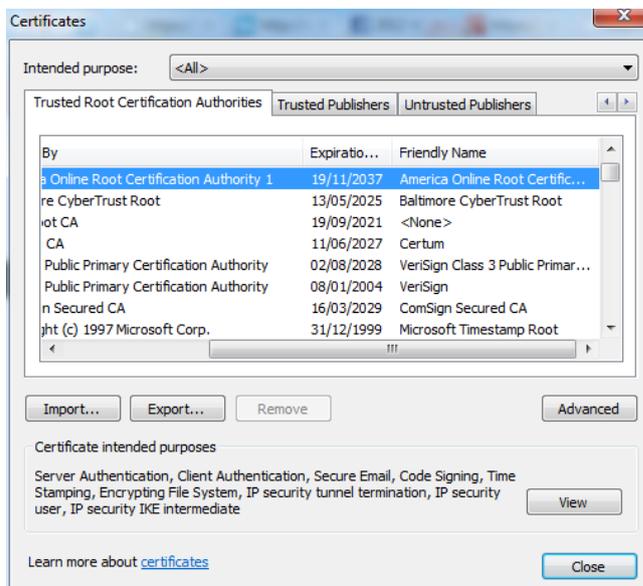
www.DigitalWhisper.co.il

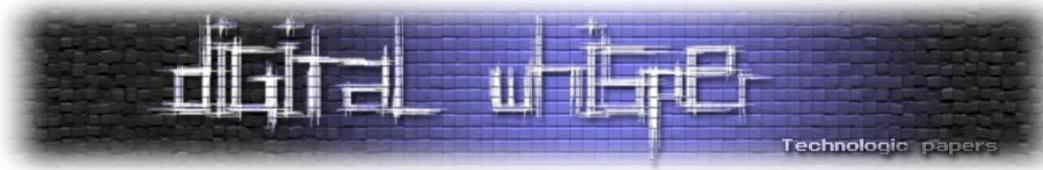
אפשר סיכום ביניים קצר?

כן. עד כה למדנו על 2 אפשרויות להחליף מפתח הצפנה בין דיפי להלמן בשביל להצפין עם מפתח ההצפנה את התעבורה. בשיטת החלפת המפתחות של דיפי-הלמן, המפתח נוצר באמצעות חישוב המפתחות של שני הצדדים, ואיתו מצפינים את התעבורה באמצעות צופן סימטרי. בשימוש באלגוריתם RSA, הגולש מגריל מספר שישמש כמפתח ההצפנה (במילים אחרות: בוחר מספר אקראי) מצפין אותו עם המפתח הציבורי של השרת, ושולח אותו לשרת. מכאן ואילך, התקשורת נעשית באמצעות מפתח ההצפנה שהגולש שלח והכל מוצפן בהצפנה סימטרית.

אז יש לנו שני אלגוריתמים, שניהם דורשים שהגולש יידע בוודאות את המפתח הציבורי של השרת כדי למנוע מתקפת MITM, איך אכן מוודאים שהמפתח לא זויף?

אה, נגעת בנקודה רגישה, אז ככה: מערכת ההפעלה באה עם רשימת מפתחות מובנית ששייכים לכל מיני חברות שנמצאות במדינות שונות ונתונות לחוקים של שלטונות שונים. כעת, כאשר דיפי רוצה לפנות לשרת של הלמן מה שהוא צריך לעשות זה לשאול את הלמן מה המפתח הציבורי שלו, לאחר מכן לשאול בצורה מוצפנת את אחד השרתים של החברות הנ"ל שנתונות תחת ממשלות שונות, האם המפתח שהוא קיבל מהלמן אכן של הלמן ואף אחד לא דחף את אפו לאמצע, אם הממשלה מאשרת, סימן שזה נכון. אני חוזר - אם הממשלה מאשרת, סימן שזה נכון. את ההמשך אנחנו יודעים, כעת כשיש לו את המפתח הציבורי של הלמן, הוא מצפין איתו מפתח ההצפנה, שולח להלמן ואז עובר להצפנה סימטרית באמצעות מפתח ההצפנה ואיתה מצפין את יתר התעבורה. הלמן שזה עתה קיבל את מפתח ההצפנה שדיפי רוצה לתקשר באמצעותו, מצפין ומפענח בהתאם את התעבורה בינו לבין דיפי.





אז כל אחת מהחברות המקושרות יכולה לפענח את התעבורה כי אני סומך עליה?
זו חולשה נוספת במנגנון ה-SSL, כפי שהוא מיושם כיום, שלא רק שכל אחת מהחברות שהמפתח שלהן מותקן כברירת מחדל על המחשב בתור Root CA יכולה לפענח את כל התעבורה, (כמובן שבמדינה מתוקנת, זו עבירה על החוק, כיוון שהיא דורשת התערבות בתעבורה ומסירת מפתח פומבי מזויף) אלא שגם כל מי שגונב ממנה את המפתח הפרטי שלה יכול...

וזו קורה בימינו?

תשאל את חבר שלי (Google) לגבי Veri-sign.

נחזור לנושא ההצפנה, למה פתאום הכנסת הצפנה סימטרית גם בצופן RSA, למה שהגולש לא יעביר באמצעות הצפנה א-סימטרית את המפתח הציבורי שלו לשרת וכך כל אחד יצפין את התעבורה בצופן א-סימטרי עם המפתח הציבורי של השני?
Performance. להצפין ולפענח בשיטת הצפנה א-סימטרית דורשת הרבה יותר משאבים מאשר הצפנה בשיטה סימטרית.

יש עוד החלטות שקשורות לביצועים?

יאפ. אורך מפתח ההצפנה.

פרט, בבקשה.

יותר קל להצפין ולפענח באמצעות מפתח קצר, ולכן בתחילת הדרך אורך המפתחות היה 40 ביט, עד שראו שזה לא מספיק חזק בהתחשב באמצעי המחשוב המתקדמים, כיוון שהתוקף יכול לנסות את כל האפשרויות עד שהוא יצליח לפענח את התעבורה. לכן פיתחו תמיכה במפתחות ארוכים יותר.

והפסיקו את התמיכה במפתחות חלשים?

מה פתאום, יש 2 עקרונות "חשובים":

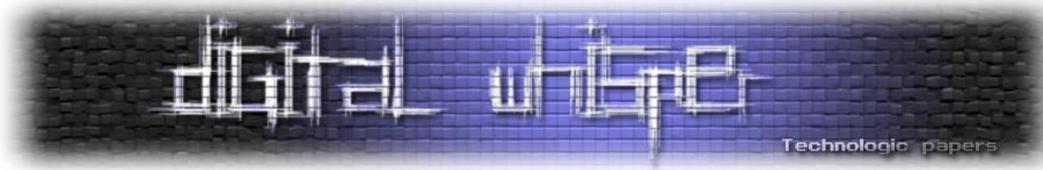
1. עובד? - אל תיגע!

2. תמיכה לאחור.

שני עקרונות חשובים אלה מוודאים שתמיד ניתן יהיה להתחבר עם מפתח חלש.

מריח כמו בעיית אבטחה...

כמובן. בתהליך ההצפנה הגולש שולח לשרת את הפרוטוקולים שהוא יודע לתקשר באמצעותם ומתוכם השרת בוחר באיזה להשתמש. אם הן השרת והן הגולש תומכים גם בפרוטוקול מאובטח וגם באחד חלש יותר, התוקף יכול לשנות את הרשימה שהגולש שולח ולהשאיר שם רק את הפרוטוקול החלש. השרת שיחשוב שזה הפרוטוקול היחיד שהגולש תומך בו, ישתמש בו להצפנת התעבורה. כעת מה שנותר לתוקף



זה לנסות את כל האפשרויות שיכולות להיות. אם נניח אורך המפתח הוא 40 ביט, יש 2^{40} אפשרויות לערכו של המפתח. רק לשם הבנה, מדובר על:

1,099,511,627,776

אפשרויות. למפתח באורך 128 ביט יש (2^{128}) :

340,282,366,920,938,463,463,374,607,431,768,211,456

אפשרויות. מינימום אורך המפתח שמקובל כיום כמאובטח הוא 128 ביט.

חזקות נוספות של המספר 2, ניתן למצוא כאן:

http://en.wikipedia.org/wiki/Power_of_two

במקרה והתוקף לא מתערב בשלב בחירת סוג ההצפנה, האם השרת בוחר את מפתח ההצפנה הכי ארוך / הכי קצר?

סוג ההצפנה ואורך המפתח הדיפולטיבי נקבע בשרת בהתאם לקנפוג, כמובן שניתן למצוא אתרים שמתעדפים מפתחות קצרים, כך שגם אם התוקף מגיע אחרי ה-Hand shake הוא יוכל לפצח/למצוא את מפתח ההצפנה עקב כך שהשרת בחר מפתח קצר ו/או פרוטוקול פגיע.

אוקיי, מה בדבר בעיות אבטחה?

RSA, דיפי והלמן, הכל טוב ויפה, אבל צריך לממש אותם, וכידוע - נדיר למצוא משהו בלי באגים. SSLv1 לא פורסם פומבית מעולם, אז אין מה להזכיר אותו. SSLv2 עדיין נתמך לצערנו בשרתים רבים למרות שנדיר למצוא דפדפנים / אפליקציות שלא תומכות ב-SSLv3.

אתה בעצם אומר ש-SSLv2 מכיל מספר בעיות אבטחה ולכן הוא פסול לגמרי? אכן.

אז תן סיכום ביניים לגבי החולשות שראינו עד כה ב-SSL.

ובכן, כעת אתה אמור להבין את הרשימה הבאה:

- תמיכה בהחלפת מפתחות בשיטת ADH (Anonymous Diffie Hellman)
- תמיכה ב-SSLv2
- תמיכה במפתחות קצרים מ-128 ביט
- תעודף של הצפנות חלשות

חולשות ב-SSL

www.DigitalWhisper.co.il

- וכמובן שאם מפתח פרטי של אחת מהחברות שמוגדרות במחשב האישי כאמינות בשביל לאמת מפתחות ציבוריים (מוכר גם כ-"תעודה" או "Certificate") דולף, ניתן לאמת באמצעותו כל תעודה בתור מקורית, כולל את של התוקף... הפתרון בכזה מקרה הוא להסיר במחשב את ה"אמון" בחברה הזו.

רשימה נאה, תביא עוד בבקשה...

אוקי. למעשה ב-SSL יש 2 הגנות, אחת מונעת קריאה של החומר (שמירה על Confidentially) ע"י גורם זר והיא ההצפנה המדוברת, השניה מונעת שינוי (שמירה על Integrity) והיא מתבצעת על ידי האשינג של חלקים / בלוקים של התעבורה. לא נאריך בנושא Hash, אני מניח ששמעת עליו. אלגוריתמים מוכרים שלו הם MD5, SHA1. במקרה הזה אין בעיה שמבוצע שימוש ב-MD5 כיוון שגם זיוף של הבלוק אולי יהיה לא קריא, אבל יהיה צורך בידיעת מפתח ההצפנה בשביל לעשות איתו משהו מעשי. בכל זאת מומלץ להשתמש ב-SHA1. גם RC4 (אלגוריתם הצפנה סימטרי) מכיל חולשות, אולם נכון להיום הוא עדיין מוגדר כחזק מספיק. למרות זאת, אם אתם נדרשים להישמע ל-FIPS, שני אלגוריתמים אלה (MD5 ו-RC4), כמו גם האלגוריתמים IDEA ו-Blowfish, נחשבים ל"ישנים" ולכן אין להשתמש בהם. בחלק של הצפנות סימטריות, רק האלגוריתמים 3DES-EDE ו-AES מאושרים ע"י FIPS. (למידע נוסף: <http://csrc.nist.gov/publications/nistpubs/800-52/SP800-52.pdf>).

בנוסף, בשביל מקרי דיבאגינג וסיבות שונות, שרתים תומכים ב-Clear text encryption, או אם תרצה סוג הצפנה: Null. זה אומר שהבלוקים לא עוברים הצפנה, אלא רק האשינג.

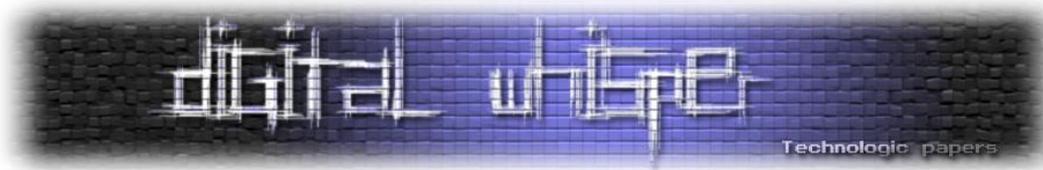
אתה לגמרי שופע הפתעות היום!

יאפ, שופע הפתעות תמיד. תעקוב מספיק תגלה 0-days מפעם לפעם...

לדוגמא?

BEAST attack, מתקפה שיצאה ב-2011 על פרוטוקולי הצפנה CBC (Cipher block chaining), בעברית מדוברת הכוונה להצפנה לפי בלוקים בגודל קבוע, להבדיל מהצפנה של Streaming שבה ההצפנה לא נעשית לפי אורכי בלוקים קבועים). במתקפה זו החוקרים ניצלו באג (שמאפשר לעקוף SOP) בפלאש שבדפדפן, שבאמצעותה יכלו ליצור ושוב ושוב בקשות HTTP מותאמות אישית לדומיין המותקף. כעת ניצלו באג בצורה שבה מומש CBC ב-SSLv3 ו-TLSv1 והצליחו באמצעות Brute Force (בעברית: כח גס, בעברית מדוברת: ניסוי כל האפשרויות) למצוא את כל פרטי הבקשה, כשמבחינתנו החלק המעניין בבקשה הוא תוכן הכותר (Header) Cookie. הבאג בפלאש תוקן, הבאג בפרוטוקול עדיין לא, ב-TLS1.1 ומעלה הבעיה לא קיימת. TLS זה השם החדש של SSL, TLS1 מגיע אחרי SSL3.

אז תוסיף לרשימת הבעיות: שימוש בהצפנה עם CBC (יש להבדיל אותו מ-CBC3 שאינו פגיע).



יש עוד?

בהחלט! יש עוד הרבה בנושא SSL... אבל באמת הגיע הזמן לסיים. אז הנה אחת לסיום: אמרנו שהסרבר מציג את המפתח הציבורי שלו, והגולש משתמש בתעודות שמוכרות אצלו במחשב (שייכות לחברות שונות) והוא פונה איתן לשרתים מסוימים בשביל לאמת את המפתח הציבורי / תעודת ה-SSL. בפועל, האימות לא נעשה לכל התעודה / מפתח ציבורי, אלא ל-Hash (גיבוב / ערבול) של מספר מאפיינים של האתר כמו שם דומיין (ובשביל אבטלה קור: שם מתחם), תאריך תפוגה, המפתח הציבורי ועוד.

אמרת Hash, תן לי לנחש, החולשה קשורה ל-MD5...

אכן, גם MD5, וגם אורך התעודה. אם האורך קצר (מתחת ל-1024 ביט, ומאז 2010 [לפי NIST] גם 1024 נחשב לקצר ועל תעודה להיות ארוכה יותר) ו/או שיטת החתימה (Hash) הינה MD5, התוקף יוכל (בעזרת כח מחשוב לא קטן) למצוא תעודה משלו, כך שכאשר תבצע עליה פעולת ה-Hash הפלט שיוחזר יהיה זהה ל-Hash של התעודה המקורית (תופעה המכונה "התנגשות", או באנגלית: Collision) וכך התוקף יוכל "לחקות" את התעודה המקורית מבלי שתהיה לו אותה במציאות. התנגשויות הן תופעות מאוד נדירות, בייחוד באלגוריתמים אלו. על מנת לאתרן יש צורך בכח חישוב עצום! עם זאת, פורסמו בעבר מספר מקרים כאלו, כדוגמת:

<http://www.mathstat.dal.ca/~selinger/md5collision/>

חולשות, חולשות, האם הן עדיין קיימות?

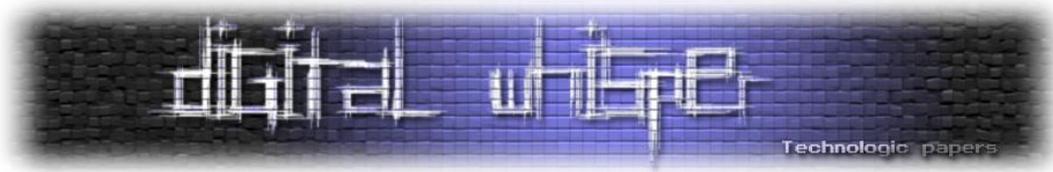
כפי שראינו קיימות מספר חולשות ב-SSL, בעיקר מדובר בשימוש בפרוטוקולים / הצפנות שנמצאו פגיעים ו/או אורך מפתחות קצר מדי. השלב העיקרי של המחקר שלי היה לבדוק האם הפרוטוקולים האלה עדיין נתמכים, והאם הן אכן מסוכנים.

מבחינת מה שבדקתי, לקחתי כתשתית WAMP 2.2 (הגרסה הכי עדכנית, נכון להיום) שמכיל Apache 2.4.2. במקביל לקחתי גם Windows server 2008 שמגיע עם IIS7 (יצוין שכבר קיים IIS 8, אבל הוא חדש ונפוץ בערך כמו Windows 8).

התקנות:

על מנת להתקין SSL על Wamp, ניתן להשתמש במדריך המצוין:

<http://forum.wampserver.com/read.php?2,32986>



כדי להתקין SSL על IIS7, ניתן להשתמש במדריך המצוין גם הוא (אני משתדל להשתמש רק במדריכים מצויינים...):

<https://learn.iis.net/page.aspx/144/how-to-set-up-ssl-on-iis/>

קנפוג:

ב-WAMP, תקנפוג את ה-SSL של Apache בקובץ:

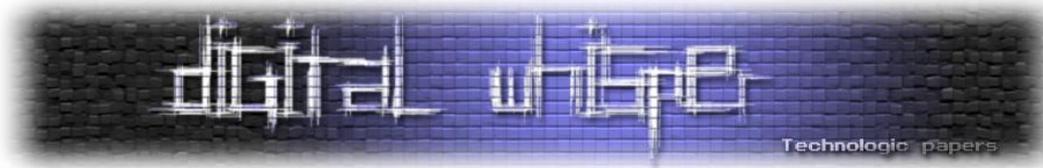
```
wamp\bin\apache\apache2.4.2\conf\extra\httpd-ssl.conf
```

בשורה SSLCipherSuite. סוגי ההצפנות המוזכרות שם מופרדות באמצעות נקודתיים. אם בתחילת השם מופיע סימן קריאה זה אומר לא לאפשר את ההצפנה המוזכרת. לדוג' השורה הבאה, מורה לשרת לאפשר את ההצפנות המוגדרות בקטגורייה Low ולא לאפשר את שיטות ההצפנה המשתמשות ב-MD5:

```
SSLCipherSuite LOW:!MD5
```

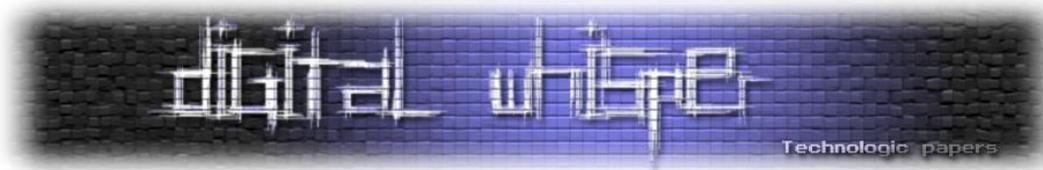
בווינדוס מגדירים הכל ב-Registry, אפשר לחפור לבד (לינק לא שימושי, אני מביא אותו רק בשביל הפרוטוקול - <http://support.microsoft.com/kb/245030>) או להשתמש בכלי גרפי:

<https://www.nartac.com/Products/IISCrypto/Default.aspx>



והתוצאה (באדום מסומנים הבעייתיים):

IIS7	APACHE 2.4.2
<p>Supported Server Cipher(s):</p> <p>Accepted SSLv2 168 bits DES-CBC3-MD5</p> <p>Accepted SSLv2 128 bits RC4-MD5</p> <p>Accepted SSLv3 168 bits DES-CBC3-SHA</p> <p>Accepted SSLv3 128 bits RC4-SHA</p> <p>Accepted SSLv3 128 bits RC4-MD5</p> <p>Accepted TLSv1 256 bits AES256-SHA</p> <p>Accepted TLSv1 128 bits AES128-SHA</p> <p>Accepted TLSv1 168 bits DES-CBC3-SHA</p> <p>Accepted TLSv1 128 bits RC4-SHA</p> <p>Accepted TLSv1 128 bits RC4-MD5</p> <p>Prefered Server Cipher(s):</p> <p>SSLv2 168 bits DES-CBC3-MD5</p> <p>SSLv3 128 bits RC4-SHA</p> <p>TLSv1 128 bits AES128-SHA</p>	<p>Supported Server Cipher(s):</p> <p>Accepted SSLv3 256 bits DHE-RSA-AES256-SHA</p> <p>Accepted SSLv3 256 bits AES256-SHA</p> <p>Accepted SSLv3 128 bits DHE-RSA-AES128-SHA</p> <p>Accepted SSLv3 128 bits AES128-SHA</p> <p>Accepted SSLv3 168 bits EDH-RSA-DES-CBC3-SHA</p> <p>Accepted SSLv3 168 bits DES-CBC3-SHA</p> <p>Accepted SSLv3 128 bits RC4-SHA</p> <p>Accepted TLSv1 256 bits DHE-RSA-AES256-SHA</p> <p>Accepted TLSv1 256 bits AES256-SHA</p> <p>Accepted TLSv1 128 bits DHE-RSA-AES128-SHA</p> <p>Accepted TLSv1 128 bits AES128-SHA</p> <p>Accepted TLSv1 168 bits EDH-RSA-DES-CBC3-SHA</p> <p>Accepted TLSv1 168 bits DES-CBC3-SHA</p> <p>Accepted TLSv1 128 bits RC4-SHA</p> <p>Prefered Server Cipher(s):</p> <p>SSLv3 256 bits DHE-RSA-AES256-SHA</p> <p>TLSv1 256 bits DHE-RSA-AES256-SHA</p>
<p>תומך ב-SSLv2. אבל אפשר לדון אותו לקו זכות, שזה שרת שיצא לפני 4 שנים, בכל זאת... סה"כ, ממש בטוח. והי, הוא לא תומך ב-CBC.</p>	<p>יחסית למצב גרוע יותר, זה סביר...</p>



ננתח את הנתונים הנ"ל באמצעות רשימת הבעיות המוכרות לנו, ונראה איזה מהם מצאנו קיימים בברירת מחדל:

חולשה	בברירת מחדל ב-Apache 2.4.2	בברירת מחדל ב-IIS7
תמיכה ב-SSLv2	לא פגיע	פגיע
תמיכה ב-ADH	לא פגיע	לא פגיע
תמיכה במפתחות קצרים מ-128 ביט	לא פגיע	לא פגיע
תעדוף (preferred) של הצפנות חלשות	לא פגיע	לא פגיע
Beast attack	פגיע	לא פגיע
Null/Clear-text encryption	לא פגיע	לא פגיע

עכשיו נראה מה קורה אם מישהו מחליט להפעיל בשרתים תמיכה בכל הצפנות, עד כמה אחראי הרשת יכול לירות לעצמו ברגל:

IIS7	APACHE 2.4.2
Supported Server Cipher(s): Accepted SSLv2 168 bits DES-CBC3-MD5 Accepted SSLv2 128 bits RC4-MD5 Accepted SSLv3 168 bits DES-CBC3-SHA Accepted SSLv3 128 bits RC4-SHA Accepted SSLv3 128 bits RC4-MD5 Accepted TLSv1 256 bits AES256-SHA Accepted TLSv1 128 bits AES128-SHA Accepted TLSv1 168 bits DES-CBC3-SHA Accepted TLSv1 128 bits RC4-SHA Accepted TLSv1 128 bits RC4-MD5 Preferred Server Cipher(s): SSLv2 168 bits DES-CBC3-MD5 SSLv3 128 bits RC4-SHA TLSv1 128 bits AES128-SHA	Supported Server Cipher(s): Accepted SSLv3 256 bits ADH-AES256-SHA Accepted SSLv3 256 bits DHE-RSA-AES256-SHA Accepted SSLv3 256 bits AES256-SHA Accepted SSLv3 128 bits ADH-AES128-SHA Accepted SSLv3 128 bits DHE-RSA-AES128-SHA Accepted SSLv3 128 bits AES128-SHA Accepted SSLv3 168 bits ADH-DES-CBC3-SHA Accepted SSLv3 56 bits ADH-DES-CBC-SHA Accepted SSLv3 40 bits EXP-ADH-DES-CBC-SHA Accepted SSLv3 128 bits ADH-RC4-MD5 Accepted SSLv3 40 bits EXP-ADH-RC4-MD5 Accepted SSLv3 168 bits EDH-RSA-DES-CBC3-SHA Accepted SSLv3 56 bits EDH-RSA-DES-CBC-SHA Accepted SSLv3 40 bits EXP-EDH-RSA-DES-CBC-SHA Accepted SSLv3 168 bits DES-CBC3-SHA Accepted SSLv3 56 bits DES-CBC-SHA

חולשות ב-SSL

www.DigitalWhisper.co.il

	<p>Accepted SSLv3 40 bits EXP-DES-CBC-SHA</p> <p>Accepted SSLv3 128 bits IDEA-CBC-SHA</p> <p>Accepted SSLv3 40 bits EXP-RC2-CBC-MD5</p> <p>Accepted SSLv3 128 bits RC4-SHA</p> <p>Accepted SSLv3 128 bits RC4-MD5</p> <p>Accepted SSLv3 40 bits EXP-RC4-MD5</p> <p>Accepted TLSv1 256 bits ADH-AES256-SHA</p> <p>Accepted TLSv1 256 bits DHE-RSA-AES256-SHA</p> <p>Accepted TLSv1 256 bits AES256-SHA</p> <p>Accepted TLSv1 128 bits ADH-AES128-SHA</p> <p>Accepted TLSv1 128 bits DHE-RSA-AES128-SHA</p> <p>Accepted TLSv1 128 bits AES128-SHA</p> <p>Accepted TLSv1 168 bits ADH-DES-CBC3-SHA</p> <p>Accepted TLSv1 56 bits ADH-DES-CBC-SHA</p> <p>Accepted TLSv1 40 bits EXP-ADH-DES-CBC-SHA</p> <p>Accepted TLSv1 128 bits ADH-RC4-MD5</p> <p>Accepted TLSv1 40 bits EXP-ADH-RC4-MD5</p> <p>Accepted TLSv1 168 bits EDH-RSA-DES-CBC3-SHA</p> <p>Accepted TLSv1 56 bits EDH-RSA-DES-CBC-SHA</p> <p>Accepted TLSv1 40 bits EXP-EDH-RSA-DES-CBC-SHA</p> <p>Accepted TLSv1 168 bits DES-CBC3-SHA</p> <p>Accepted TLSv1 56 bits DES-CBC-SHA</p> <p>Accepted TLSv1 40 bits EXP-DES-CBC-SHA</p> <p>Accepted TLSv1 128 bits IDEA-CBC-SHA</p> <p>Accepted TLSv1 40 bits EXP-RC2-CBC-MD5</p> <p>Accepted TLSv1 128 bits RC4-SHA</p> <p>Accepted TLSv1 128 bits RC4-MD5</p> <p>Accepted TLSv1 40 bits EXP-RC4-MD5</p> <p>Prefered Server Cipher(s):</p> <p>SSLv3 256 bits ADH-AES256-SHA</p> <p>TLSv1 256 bits ADH-AES256-SHA</p>
--	---

חולשות ב-SSL

<p>לא טעיתם, הרשימה הזו זהה לחלוטין לרשימה הקודמת. בברירת מחדל ב-IIS7 כל האפשרויות הנתמכות מופעלות...</p>	<p>שימו לב לפרוטוקולים המומלצים. למרות זאת, זה לא משנה הרבה כי ב-ADH, אם התוקף מתערב בתעבורה אחרי שהתחילה התקשורת זה מאוחר מדי - הצדדים כבר החליפו מפתחות. ואם הוא מתערב בתעבורה לפני שהתחילה התקשורת, הוא יכול לעקוף את הגדרות ההעדפה שבשרת כמו שהוזכר לעיל.</p>
---	---

ושב ננתח את הנתונים הנ"ל באמצעות רשימת הבעיות המוכרות לנו, ונראה איזה מהם מצאנו שאפשריים בשרתים הללו:

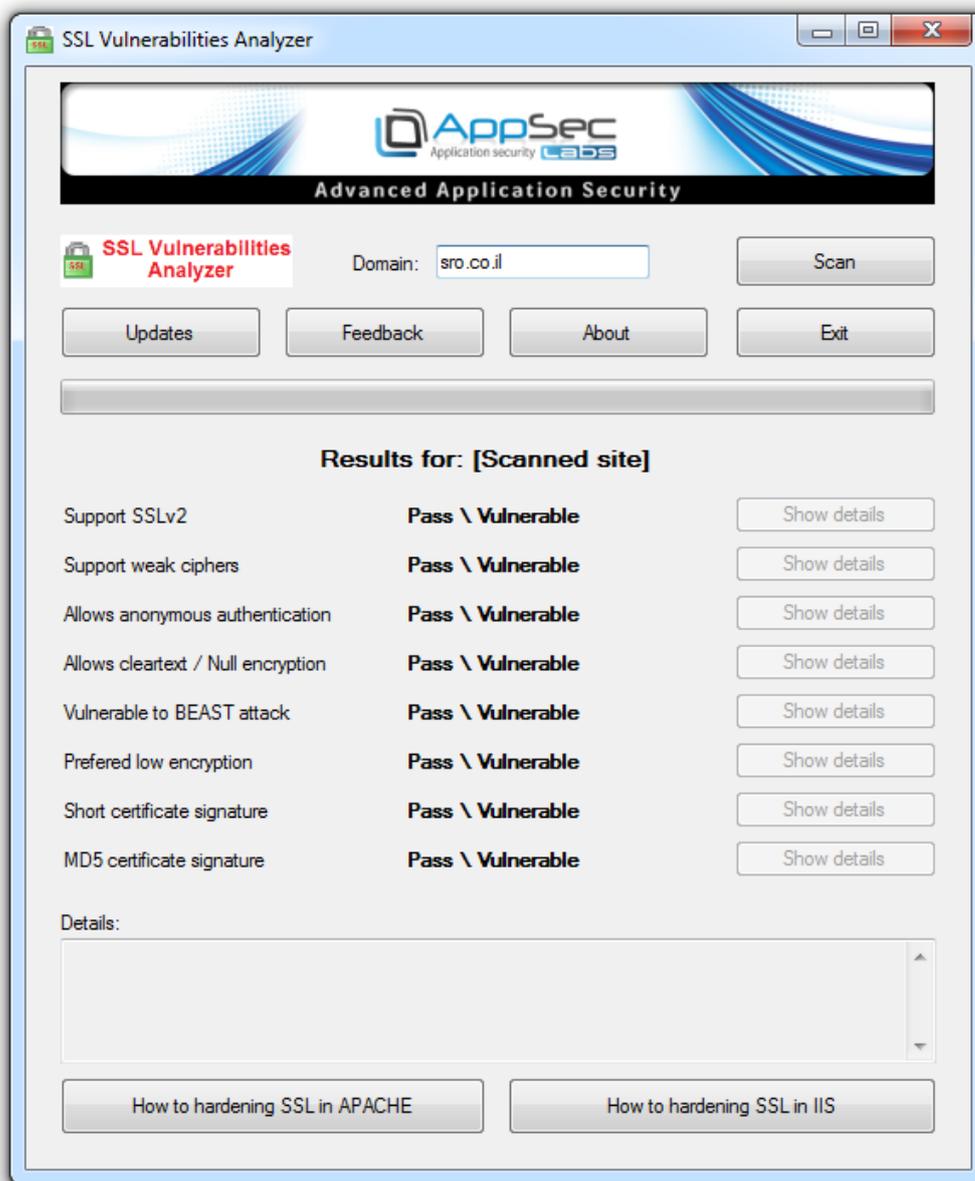
אפשרי ב-IIS7	אפשרי ב-Apache 2.4.2	חולשה
כן	לא	תמיכה ב-SSLv2
לא	כן	תמיכה ב-ADH
לא	כן	תמיכה במפתחות קצרים מ-128 ביט
לא	כן	תעדוף (preferred) של הצפנות חלשות
לא	כן	Beast attack
לא	לא	Null/Clear-text encryption

ברשימת ההצפנות שנתמכות בשרתים אחרים ו/או גרסאות ישנות יותר, ניתן לצפות כאן:

http://www9.atwiki.jp/kurushima/pub/pkimisc/SSLTLS_CipherSuite_Support_Table_.html

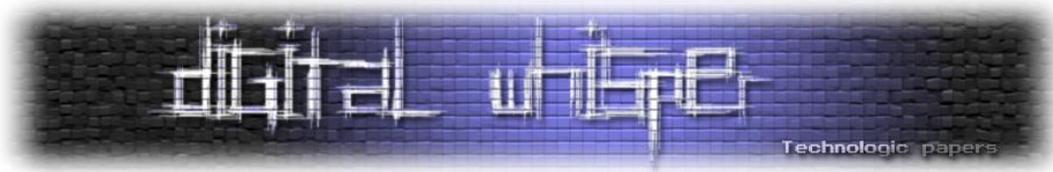
SSL vulnerabilities analyzer tool

השלב הבא הוא כתיבת כלי שמבצע לכל הניתוח הנ"ל אוטומציה ומציג תוצאה ברורה, אז עשיתי את זה...
כתבתי כלי גרפי נאה, שמקבל דומיין / IP ומנתח בצורה ברורה את הצפנות ה-SSL שהוא תומך בהם:



הכלי ניתן להורדה בכתובת:

https://appsec-labs.com/SSL_Analyzer



עד כמה אתם החולשות מסוכנות?

לאחר שסיימתי את השלב הראשון - לימוד החולשות, השלב השני - כתיבת כלי (חוקי, חוקי, אני פנטסטר), פניתי לבדוק עד כמה החולשות אכן מסוכנות.

הגדרתי את השרתים שיתמכו רק בהצפנות פגיעות, ב-IIS זה היה ע"י חסימה של SSL3 ו-TLS, והפעלת תמיכה ב-SSL2, הכל ברג'יסטרי. ב-APACHE הגדרתי בקובץ httpd-ssl.conf:

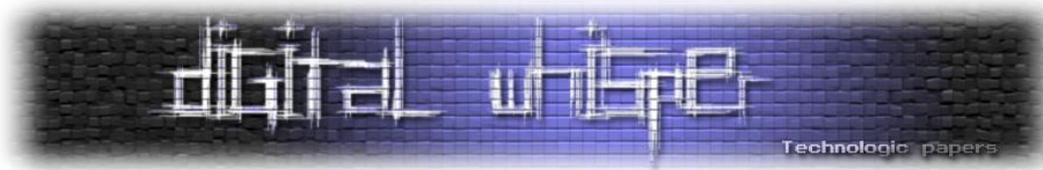
```
SSLCipherSuite ADH-AES256-SHA:ADH-AES128-SHA:ADH-DES-CBC3-SHA:ADH-DES-CBC-SHA:EXP-ADH-DES-CBC-SHA:ADH-RC4-MD5:EXP-ADH-RC4-MD5:EDH-RSA-DES-CBC-SHA:EXP-EDH-RSA-DES-CBC-SHA:DES-CBC-SHA:EXP-DES-CBC-SHA:IDEA-CBC-SHA:EXP-RC2-CBC-MD5:EXP-RC4-MD5:ADH-AES256-SHA:ADH-AES128-SHA:ADH-DES-CBC3-SHA:ADH-DES-CBC-SHA:EXP-ADH-DES-CBC-SHA:ADH-RC4-MD5:EXP-ADH-RC4-MD5:EDH-RSA-DES-CBC-SHA:EXP-EDH-RSA-DES-CBC-SHA:DES-CBC-SHA:EXP-DES-CBC-SHA:IDEA-CBC-SHA:EXP-RC2-CBC-MD5:EXP-RC4-MD5:DES-CBC3-MD5:RC4-MD5
```

פתחתי Chrome, FF, IE, Opera וגולשתי לשרתים ב-https. כפי שניתן לראות בטבלה למעלה, כל הדפדפנים שנבדקו הציגו חזית אחידה וחסמו את כל הפרוטוקולים הפגיעים. כרום ופיירפוקס הציגו שגיאה מובנת, IE ו-Opera הציגו דף דיפולטיבי והשגיאה הופיעה רק ב-title.

דפדפנים פגיעים?	נתמך ב-Apache2.4?	נתמך ב-IIS7?	הצפנה
X	V	X	Accepted SSLv3 256 bits ADH-AES256-SHA
X	V	X	Accepted SSLv3 128 bits ADH-AES128-SHA
X	V	X	Accepted SSLv3 168 bits ADH-DES-CBC3-SHA
X	V	X	Accepted SSLv3 56 bits ADH-DES-CBC-SHA
X	V	X	Accepted SSLv3 40 bits EXP-ADH-DES-CBC-SHA
X	V	X	Accepted SSLv3 128 bits ADH-RC4-MD5
X	V	X	Accepted SSLv3 40 bits EXP-ADH-RC4-MD5
X	V	X	Accepted SSLv3 56 bits EDH-RSA-DES-CBC-SHA
X	V	X	Accepted SSLv3 40 bits EXP-EDH-RSA-DES-CBC-SHA
X	V	X	Accepted SSLv3 56 bits DES-CBC-SHA
X	V	X	Accepted SSLv3 40 bits EXP-DES-CBC-SHA
X	V	X	Accepted SSLv3 128 bits IDEA-CBC-SHA
X	V	X	Accepted SSLv3 40 bits EXP-RC2-CBC-MD5
X	V	X	Accepted SSLv3 40 bits EXP-RC4-MD5

חולשות ב-SSL

www.DigitalWhisper.co.il

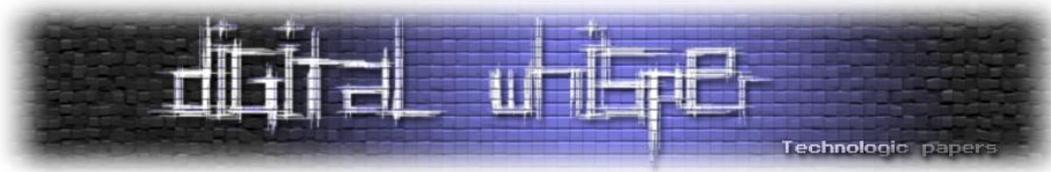


X	V	X	Accepted TLSv1 256 bits ADH-AES256-SHA
X	V	X	Accepted TLSv1 128 bits ADH-AES128-SHA
X	V	X	Accepted TLSv1 168 bits ADH-DES-CBC3-SHA
X	V	X	Accepted TLSv1 56 bits ADH-DES-CBC-SHA
X	V	X	Accepted TLSv1 40 bits EXP-ADH-DES-CBC-SHA
X	V	X	Accepted TLSv1 128 bits ADH-RC4-MD5
X	V	X	Accepted TLSv1 40 bits EXP-ADH-RC4-MD5
X	V	X	Accepted TLSv1 56 bits EDH-RSA-DES-CBC-SHA
X	V	X	Accepted TLSv1 40 bits EXP-EDH-RSA-DES-CBC-SHA
X	V	X	Accepted TLSv1 56 bits DES-CBC-SHA
X	V	X	Accepted TLSv1 40 bits EXP-DES-CBC-SHA
X	V	X	Accepted TLSv1 128 bits IDEA-CBC-SHA
X	V	X	Accepted TLSv1 40 bits EXP-RC2-CBC-MD5
X	V	X	Accepted TLSv1 40 bits EXP-RC4-MD5
X	X	V	Accepted SSLv2 168 bits DES-CBC3-MD5
X	X	V	Accepted SSLv2 128 bits RC4-MD5

הדפדפנים היו כמעט כולם גרסאות עדכניות. כך שאם הדפדפן שלכם מעודכן, אתם מוגנים ממנהלי רשת לא אחראיים.

נ.ב. למי שממש רוצה שהדפדפן שלו יתמוך בפרוטוקולים חלשים, ניתן לבצע זאת בדרך כלל. לדוגמא:

<http://www.techbug.com/en/knowledge-base/firefox-cant-connect-securely-to-url-because-the-site-uses-a-security-protocol-which-isnt-enabled/>



לינקים לקריאה נוספת

SSL Protocol: http://en.wikipedia.org/wiki/Transport_Layer_Security

SSL Protocol: <http://technet.microsoft.com/en-us/library/cc767139.aspx>

OWASP Testing Guide: [https://www.owasp.org/index.php/Testing_for_SSL-TLS_\(OWASP-CM-001\)](https://www.owasp.org/index.php/Testing_for_SSL-TLS_(OWASP-CM-001))

Beast attack: <https://isc.sans.edu/diary.html?storyid=11722>

לסיכום

במאמר זה סקרתי בקצרה מגוון תחומי אבטחה בהקשר של SSL, החל מהסברים על שיטות ההצפנה והחלפת המפתחות, המשך בסקירת חולשות שונות הקשורות ל-SSL, סקירת הכלי sslscan וניתוח תוצאותיו, הצגת הכלי שפיתחתי SSL Vulnerabilities Analyzer שמנתח באופן ברור ונאה את החולשות שקשורות ב-SSL בשרתים. התקדמתי לקראת סיום בבדיקת האלגוריתמים שנתמכים בשני סוגי שרתים פופולריים ולסיום הראיתי שנכון להיום, מי שגולש בדפדפן מודרני מעודכן (מאלה שנבדקו) מוגן מפני אלגוריתמים פגיעים אלה.

במאמר הבא אסקור את שפות התוכנה, איך והאם הן מתמודדות עם אלגוריתמים חלשים ב-SSL ו/או חותמים לא מוכרים. האם אכן VBS מאובטח יותר מפייתון?.. על כך ועוד, המתינו לחלק הבא.

כל הנ"ל ניתן להרחבה וחלקים שונים נמצאים במחקר מתקדם. תרגישי/ חופשי להשאיר פידבק (israel@appsec-labs.com), תודה מראש. אני שמח לתרום את המאמר לקהילה, ומקווה שהתרומה הישראלית לקהילה הישראלית תתרחב.

ישראל חורז'בסקי [Sro.co.il]

ראש צוות Penetration Testing ב-AppSec Labs

זיהוי אנשים ומטופלים על פי מבנה כף יד ורנטגן

מאת אמיתי דן

הקדמה

מה הייתם מעדיפים, פרטיות טובה יותר או אבחון רפואי וטיפול טוב יותר? במאמר זה אסקור קונפליקט בין רפואה ופרטיות, ואנסה לחשוב (בקול רם) להיכן הטכנולוגיה שאני נחשפתי אליה יכולה לקחת אותנו עוד תקופה לא ארוכה.

לפני כמה שנים התחילו להציע בנתב"ג לנוסעים לעבור למסלול הבידוק המהיר, מסלול זה אשר אפשר לעבור הליך הרשמה ולהשתמש במכשיר המזהה את הנוסע לפי מבנה כף היד שלו וזאת ללא צורך בטביעות אצבעות ובכך לעבור ביקורת דרכונים ללא תור.

הטכנולוגיה שעליה המכשירים נשענים, מתבססת על המבנה הייחודי של כף היד שלנו המאפשרים לנו לזהות אנשים על פי פרופורציות כף היד. השיטות האמינות כיום בתחום זה נקראות "Palm Geometry" ו-"Hand Geometry", השימוש בהן מתבצע פעמים רבות תוך שילוב בין שתי השיטות. טכנולוגיות אלו היו בשימוש הרבה שנים לאחור, ולמרות שטביעות אצבעות אינן דבר חדש כלל, השימוש בשיטות ביומטריות של זיהוי גיאומטרי של מבנה כף יד לצורך בקרת כניסה או יציאה, זיהוי מיידי של אנשים נכנסו לשימוש הרבה לפני בקרות הכניסה מבוססות מערכות לזיהוי טביעות האצבעות כמזהה ביומטרי יחיד.

חשיפת פרטים רפואיים לצורך לימוד

באופן אישי, כאחד המתעסק בספורט אתגרי מגיל צעיר יצא לי לא פעם להיחבל ולכן מצאתי את עצמי עובר בדיקות רדיולוגיות שונות. בדיקות אלו לעיתים היו במסגרת מרפאות של קופת החולים, אך לא פעם מצאתי את עצמי מקבל שירותים במרפאות חירום פרטיות המעניקות שירות לחברי קופות החולים מתוך הסכמים של הקופות עם המכונים הפרטיים.

הסיפור שלי התחיל כשיום אחד גיליתי שהפרטיות המטופלים לא נשמרת, ומערכת לימודית רפואית חושפת את הפרטים של המטופלים לצרכים לימודיים.

מה שהתרחש וגרם לי לפקוח את העיניים, היה, שתצלומי הרנטגן של המטופלים הועלו לצרכים לימודיים רפואיים, וכך לצורך אקט שהינו חיובי ומובן (רופאים מנוסים יותר שיתנו טיפול טוב יותר) מפורסמים נתונים רפואיים של מטופלים.

זיהוי אנשים ומטופלים על פי מבנה כף יד ורנטגן

www.DigitalWhisper.co.il

חשוב לציין שאת כתובת האתר ניתן לאתר בעזרת חיפוש בגוגל או באתרים בעלי רקע דומה, הוא מאפשר לכל אדם להירשם אליו ולאחר הרשמה קצרה הדורשת אימייל שם משתמש סיסמא ושם פרטי ומשפחה, ניתן להתחבר למערכת בצורה רגילה.

הנתונים מוגנים מזיהוי מיידי, וברוב המוחלט של המקרים לא מצוינים שם שמות, אבל יש שם אזהרה שאם מועלת תמונה עם זיהוי יש לדווח למנהל האתר באופן מיידי. אזהרה זו גרמה לי להבין שלעיתים קורה שמועלות לשם תמונות רנטגן עם תעודות זהות, ולכן כדאי לבדוק האם נשאר פרטים על תמונות הקיימות במאגר.

הדברים שכן קיימים במערכת לימודית הם גילאים ולעיתים גם הרקע של החבלה או הפציעה ומין הפצוע. מצאתי תמונות מסוגים שונים ובהם תמונות החושפות איברי גוף מסוגים שונים. בין כלל התמונות, היו לא מעט תמונות של גפיים עליונים. וכאן הנושא התחיל להתפתח, וזאת מאחר שגיאומטריה של מבנה עצמות כף היד משמשת לזיהוי אישי של אדם באופן חד-חד ערכי.

כבר בשלב הראשוני כאשר ראיתי את צילומי הגוף ולפני שהבנתי שניתן לזהות אנשים על פי גיאומטריה של כף יד, שלחתי אימייל למנהל המערכת ותוך כדי התכתבות איתו נאמר לי שלדעתו חוסר אזכור שם מפורש של המטופל ותעודת זהות מהווה שמירה מספקת על הפרטיות, עקב כך קיבלתי התרשמות כללית שהגישה היא שאנשים לא אמורים לחשוב כיצד לתקוף מערכות רפואיות, וכך גם נדלקו לי נורות אדומות נוספות.

חשוב להבין שאם זיהית שם לפי המקרה שמתואר יחד עם התאריך עובד שלך, או אדם אחר (מטופל מהמרפאה) יכולת לדעת כיצד הוא נראה מבפנים מבלי להשתמש בשום טכנולוגיה נוספת.

יש לא מעט אנשים וארגונים שאוספים מידע, ויש לא מעט אנשים שמוכנים לשלם על מידע זה, כסף רב. פרסום תמונות רנטגן עם יכולת, ולו הקלושה ביותר של זיהוי הינה בעייתית, ומאחר שכאן היכולת לא קלושה ההשלכות יכולות לעורר דילמה מוסרית יחד עם פגיעה בפרטיות. אגב, אחד הדברים המעניינים הם, שיש הערה המציינת שתצלומי הרנטגן עלולים להיות מוגנים בזכויות יוצרים, בעוד שכלל לא ברור האם הפציינט אישר מלכתחילה להשתמש בתמונות של הגוף שלו.

כשהמשכתי לחקור את העניין התברר לי תוך כדי התייעצות ומחקר עצמאי שיש שיטות לא מעטות לזיהוי ביומטרי של אנשים, בין היתר על פי מבנה גוף, וההבנה שבשדות תעופה הטכנולוגיה לזיהוי גיאומטרי של מבנה יד מספיק אמינה, הבנתי שיש פה יותר מחשש לפגיעה בפרטיות של מטופלים.

חשוב להבדיל בין זיהוי של מבנה ידיים וגוף חיצוניים לבין זיהוי של המבנה תוך ניתוח של תמונת רנטגן, ולמרות זאת יש לא מעט מחקרים שעוסקים בשיטות אלו כך שלא ניתן להגיד באופן גורף שחוסר בתעודת זהות לא מהווה פגיעה בפרטיות, הרי לא כל כך מהר ניתן להחליף את מבנה הגוף, ואילו תעודת זהות הינה מספר בלבד.

זיהוי אנשים ומטופלים על פי מבנה כף יד ורנטגן

www.DigitalWhisper.co.il

ככל שהמשכתי ללמוד הבנתי שמהו בשיטת העבודה הרפואית שם אותנו המטופלים בפינה, כדי ללמוד כיצד לטפל בנו טוב יותר מחליטים ברוב המקרים ללא ידיעתנו להעלות למאגר פתוח (גם לציבור) צילומים לדוגמה וכך מי שיהיה בעל אמצעים יוכל לגלות לא רק מה מצבנו הרפואי אלא אף מה הרקע של הפציעה שגרמה לבדיקת הרנטגן.

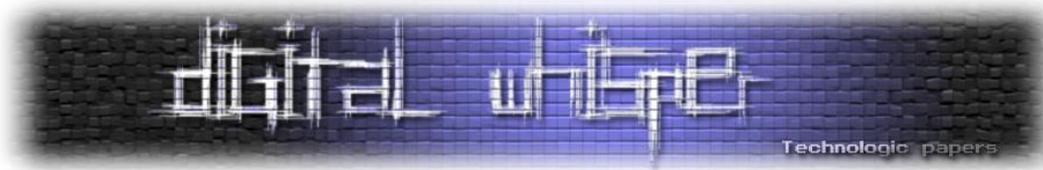
אז מה יותר חשוב? פרטיות או בריאות?

כפי שאמרתי לא מעט מחקרים עוסקים בזיהוי על פי גיאומטריה של תצלום חיצוני של כף היד (בדומה לנתב"ג) אבל אחרים עוסקים גם בזיהוי של אנשים על פי תמונות רנטגן, אישית לא הייתי רוצה לראות תמונה של הגוף שלי עם צימוד לתעודת זהות ולכן אני מנסה לעורר את הנושא. הנחתי שלא מדובר בשיטת עבודה של רופאים בישראל בלבד, אלא גם במדינות אחרות ברחבי העולם וכך חיפשתי מידע נוסף ומצאתי שהמערכת שאיתרתי בישראל (ללימוד חופשי של רופאים, ואנשים תאבי ידע) קיימת בווריאציות שונות גם במדינות אחרות. הבנה זו, שבעצם כיום קיימת תשתית מחקרית ובהתאם לאזור הגוף גם יישומית לזהות אנשים שעברו טיפול במערכות רפואיות, אשר אחריו פרטיהם נחשפו באופן שניתן לזהותם תוך השוואה לתמונה אחרת הביאה אותי להבנה שאכן יש כאן פרדוקס.

מצד אחד, כדי לנהל מחקר רפואי ולהתעדכן הרופאים חייבים להתאמן וללמוד, אחרת נקבל טיפול רפואי פחות מקצועי ומאידך, יש פה פגיעה באבטחת המידע והפרטיות של המטופלים, אני כפציינט ואחרים כמותי לא נסכים שהפרטים הרפואיים שלנו יפורסמו אם יוכלו לזהות אותנו לאחר מכן ובו בזמן נרצה שיטפלו בנו רופאים מנוסים.

אז מה יותר חשוב בעצם, אבטחת מידע ופרטיות או טיפול רפואי הולם? לא פעם שומעים שהבריאות מעל הכול ואולי כאן אין דרך אחרת אלא לבחור בהתמקצעות רפואית על פני שמירת סודיות רפואית. כדרך לפתרון, חשבתי על כך שאם פציינטים יחתמו על טופס הסכמה לשימוש בפרטיהם הרפואיים לצורך לימודי, בדומה לכרטיס אד"י וזאת תוך הבנה שבכך פרטיהם יחשפו לזיהוי, נוכל לדעת שלפחות הייתה כאן מודעות להשלכות. עד שיעשה משהו בנידון יש לקחת בחשבון שבשם החופש הרפואי והצורך בלמידה, ייתכן שבדיקת הרנטגן שלכם או מישהו שאתם מכירים מתפרסמת בצורה שניתן לשייך אותה לפציינט על ידי טכנולוגיות לזיהוי ביומטרי של תמונות רנטגן.

לא חסרים שירותים בעולם שמספקים שירותי למידה בעזרת תיקים רפואיים של תצלומי רנטגן, ורדילוגיה אחרים, לאור זאת יש לבחון את הדברים ללא התייחסות להפקרת המידע הנקודתית שאחשוף בהמשך המאמר.



בחזרה לפן הטכני, מאחר שבגוף קיימים איברים רבים, והטכנולוגיה של זיהוי ביומטרי על פי מבנה הגוף (אם על ידי תמונה חיצונית ואם על ידי ניתוח תוצאות של מכשירים רדיולוגיים, כגון: CT, MRI, X-Ray) נכנסת לשימוש יותר ויותר, הרי שיש רצון לפתח שיטות שונות לשימוש בטכנולוגיות אלו.

ביומטריה על פי מבנה גיאומטרי של עצמות ושיטות מתפתחות אחרות הינה דבר שיש להפנים ולהבין את ההשלכות שלו, החיוביות השליליות והעובדתיות. כבר כיום יש חלקי גוף שצילומי רנטגן לבדם מאפשרים זיהוי ביומטרי עם נתוני סטייה נמוכים, שקלול של תמונה פיזית יחד עם תצלום רנטגן (הרי זאת אותה יד) יאפשרו דיוק טוב יותר.

אחד מהתרחישים האפשריים לדוגמא הוא של מתאגרף או מתאמן באומנות לחימה אחרת שמתחרה בקרב יוקרתי, חדירה לנתונים הרפואיים שלו תאפשר לדעת מהי נקודת התורפה שלו, כיצד והיכן להכות וזאת בדרך לניצחון.

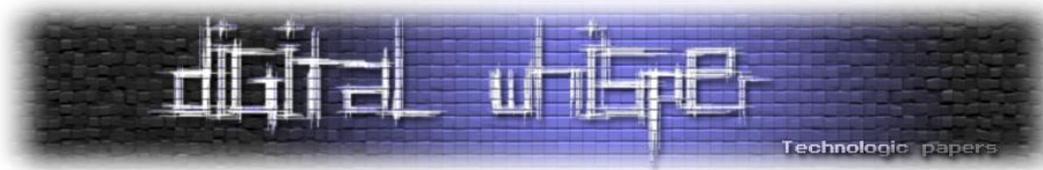
נקודות של עתידנות

לפני מספר שנים פורסם מאמר על הצלחה של קבוצה אקדמאית לשכפל מפתח על ידי צילום מרחוק, לא מזמן נחשף שנפרצו בתים בישראל בשיטה דומה אם כי תוך צילום מטווח קצר. לדעתי לא ירחק היום שניתן יהיה לזהות אנשים על פי צילומי הידיים שלהם ברחוב תוך שימוש בטכנולוגיות ישנות של זיהוי על פי מבנה גיאומטרי של מבנה כף יד שמשמשות כבר לזיהוי, וכך קבלת אימות וודאי תוך הצלבה עם נתונים נוספים כמו זיהוי פנים.

שיטה זו שתנסה לנתח את מבנה הגיאומטרי של הידיים תאפשר לזהות אנשים ממרחקים כל עוד תנחות היד מאפשרות זאת. באותה מידה לדעתי ניתן לפתח את השיטה לכך שניתן יהיה לזהות אנשים רעולי פנים (לדוגמא בזמן שוד), נפגעים וחללים, ואנשים שבלתי ניתן יהיה לקחת מהם טביעות אצבעות מסיבות שונות.

אני סבור שזיהוי ביומטרי על סמך גיאומטריה של מבנה כף היד נשאר מאחור, בעוד שטביעות אצבעות ופנים הפכו לכלים מועדפים. מאחר שכבר כיום ניתן לזהות צילומי רנטגן ולשייך אותם לאנשים אני סבור שכעת אפשר לבצע זיהוי משולב, לצבוע את תצלום הרנטגן של כף היד ולזהות את מי שהיד שייכת לו לאחר מכן.

כפי שתראו בתמונה בהמשך ניתן לזהות בבירור את מתאר העור, ולכן ניתן לשלב שיטות זיהוי, ולאחד את פענוח הרנטגן עם פענוח קווי המתאר הגיאומטריים של היד.



במחקר שערכתי על היכולת לאסוף מאגרי מידע בדרכים יצירתיות ולהלביש עליהם פנים חשבתי שאולי זיוף פנים יכול להוות פיתרון למי שיחשוש מזיהוי שלו, כאן מתברר לי שהידיים שלנו הולכות להיות קלף לא קטן בביומטריה החזותית, ושלא יצטרכו שניתן טביעות אצבעות אלא פשוט יצלמו אותנו ממרחק.

בגלל מאמר זה חשבתי שאולי יש כבר טכנולוגיה לביומטריה מרחוק בטביעות אצבעות, ואכן חברת Start up חדשנית בשם IDair יצאה לא מזמן עם מוצר המאפשר קריאת טביעות אצבעות ממרחק של 6 מטר ללא מגע.

אין סיבה שלא נוכל לבצע זאת גם בצילום איכותי מרחוק של גיאומטריית ידיים במקרה שהיד נמצאת בזווית הנכונה.

לדעתי בעתיד הלא רחוק יתאפשר למי שיחזיק בטכנולוגיה המתאימה לקרוא טביעות אצבעות ומבנה ידיים ממרחק רב יותר של מאות מטרים, וכך יתאפשר לבצע איתור זיהוי מרחוק של גורמים פליליים לאומניים ואחרים גם כאשר הפנים שלהם חשופות.

במאמר מוסגר יש לציין כי כבר כיום ניתן לזהות ביומטרית על ידי טכנולוגיות של ציטות בעזרת קרני לייזר ממרחק רב.

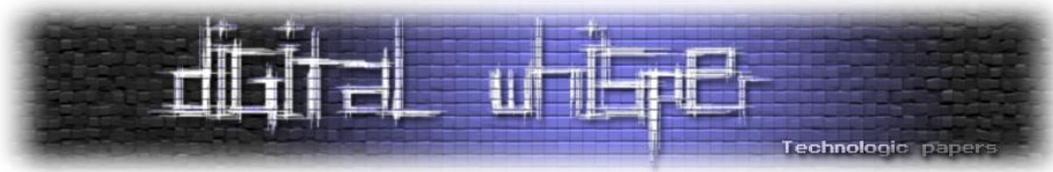
התפתחות במחקר

בזמן כתיבת שורות אלו מצאתי במאגר רפואי לימודי תמונות רנטגן עם תעודות זהות ישראליות ברורות, ככה שהמחקר שלי הפך להיות פרצת אבטחה וודאית מסוג חדש מעניין מרתק ומרתיע. אני מאמין שלפעמים כדאי לחשוב קדימה לבנות תרחישי קיצון ולהמציא בעיות, בעיות בשיטות עבודה.

לא מדובר עוד בפגיעה בפרטיות אלא ביכולת לפרסם תמונה של אדם תוך חשיפת האיברים שלו, וזה כבר משהו שאנחנו לא רגילים אליו, שוב חברה לא תוכל לבטל את החשיפה של הנתונים.

סיכום

במאמר זה הבאתי דוגמאות לטכנולוגיות בפיתוח, כאלו שכבר משתמשים בהם ואלו שאולי יגיעו, תוך הצבה מול מציאות נתונה שמתעלמת מהתפתחויות אלו. לדעתי עלינו לדרוש מהרופאים לשמור על הפרטיות שלנו, ולאזן את האינטרס של הלמידה עם האינטרס של שמירה על זכויות החולה כאזרח וכאדם.



המצב שמתקיים בתמונות שמוצגות בנספחים, שבו כבר מופקרים פרטים רפואיים הינו בלתי נסבל. כפי שצינתי, גם אם לא היו מפרסמים מספרי תעודות זהות על חלק מתמונות הרנטגן שנלקחו מחומר רפואי של מטופלים תוך פגיעה בסודיות רפואית, עדיין היו טכנולוגיות שיכלו לבצע שיוך לאדם בהינתן מצב מסוים. יש לבחון מחדש את שיטת העבודה שבה רופאים מתנסים בחומר רפואי חדש, ומתנסים לצורך מקצועי, ולבדוק האם היא לא פוגעת בפרטיות הפצינטיים מתוקף היותם אזרחים. אני סבור שגם אם יוחלט לחשוף את נתוני המטופלים חרף היכולת לזהות אותם (באמצעים ביומטריים שונים) יש לעשות זאת תוך החלטה מודעת ובשיתוף הציבור. כשחשבתי לאן אפשר לקחת את הדברים הבנתי שיתכן שנוכל לזהות גם לאחור מקרי פשע וטרור, בזמן אירועים שבהם ידיים של אנשים נחשפו וצולמו בעוד שהראש היה מוסתר.

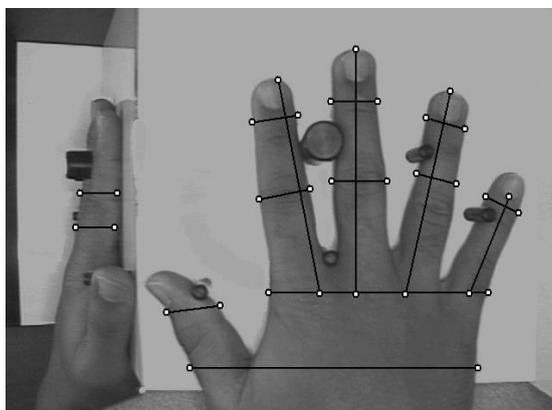
נספחים:

צילומי רנטגן מהמאגר הלימודי:

המשותף לדוגמאות הבאות הוא חשיפה פומבי של מידע רפואי יחד עם מספרי תעודות זהות של הפציינטיים, דבר המאפשר היתכנות לבצע צימוד של תעודת זהות לצילומי גוף פולשניים המהווים נתונים רפואיים. נתונים אלו מתווספים למאגרי המידע שחקרתי בעבר כחלק מבניית פרופיל על אנשים, מחקר זה פורסם בן היתר במגזין זה בגיליון 29. חיבור של כלל הנתונים שנאספו על היעד, כולל תמונה רגילה יאפשר הקרנה של מציאות רבודה בנתונים פרוצים רב תחומיים במערכות ניידות וניחות בעלות יכולת לזיהוי ביומטרי. את מספרי התעודות היה ניתן למצוא בצד שמאל למעלה אך הן טושטשו לצורך פרסומן במאמר זה:



דוגמא לזיהוי ביומטרי בעזרת גיאומטריה של כף יד:

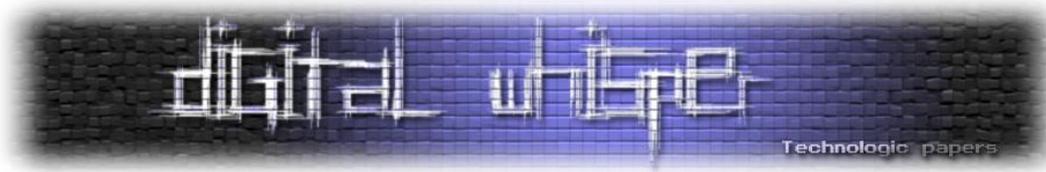


קישורים לקריאה נוספת:

- http://biometrics.cse.msu.edu/hand_proto.html
- <http://www.iaa.gov.il/Rashat/he-IL/Airports/BenGurion/InformationforTravelers/Services/BiometricSecurityCheck/>
- <http://www.ijcaonline.org/archives/volume42/number7/5704-7726>
- <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.172.7009&rep=rep1&type=pdf>
- http://www.ijens.org/Vol_12_I_01/122801-9494-IJVIPNS-IJENS.pdf
- http://kritis.coddex.com/Collage/Bsc/Ariel/Graffiti%20Detection/2_01_10/Final%20Project/Project%20Books/%E7%E6%E9%20%E2%EE%E9%E0%EC/DOCUMENTATION/%F1%F4%F8%20%E4%F4%F8%E5%E9%F7%E8%20-%20%E2%EE%F2%F8%EB%FA%20%EC%E6%E9%E4%E5%E9%20%E0%E3%ED%20%EC%F4%E9%20%F4%F8%E5%F4%E5%F8%F6%E9%FA%20%EB%F3%20%E4%E9%E3%20-%20%E7%E6%E9%20%F2%EE%E9%E0%EC%20-%2024967705.doc
- <http://diuf.unifr.ch/diva/biometrics/MyIdea/en/technology/hardware.html>
- http://perec.uoregon.edu/new_entry_procedures.html
- http://my.safaribooksonline.com/9780750679671/combining_biometric_methods#X2ludGVybmlsF5X0ZsYXNoUmVhZGVyP3htbGkPTk3ODA3NTA2Nzk2NzEvdmlpaQ==
- http://terpconnect.umd.edu/~mudit/index_files/Human%20identification%20using%20x-rays.pdf
- http://library-resources.cqu.edu.au/JFS/PDF/vol_50/iss_2/JFS2004229.pdf
- <http://www.amazon.com/Forensic-Human-Identification-Introduction-ebook/dp/B0084ETQHW>
- <http://www.cse.msu.edu/~cse891/Sect601/textbook/4.pdf>
- http://visgraph.cs.ust.hk/biometrics/Visgraph_web/AVBPA_Paper.pdf
- <https://www.google.co.il/search?q=human%20identification%20using%20x%20ray&hl=iw&biw=1024&bih=605&ie=UTF-8&sa=N&tab=iw&ei=glw5UO3PJ7CA0AXnv4CAAg>
- <https://www.google.co.il/search?q=human+identification+using+geometric&hl=iw&client=firefox-a&rls=org.mozilla:he:official&biw=1024&bih=605&prmd=imvns&source=lnms&sa=X&ei=7Yw5UMifBYfL0Qxa14C>

זיהוי אנשים ומטופלים על פי מבנה כף יד ורנטגן

www.DigitalWhisper.co.il



[wDA&ved=0CAgQ_AUoAA#hl=iw&client=firefox-a&rls=org.mozilla:he%3Aofficial&q=human+identification+using+geometric+xray&oq=human+identification+using+geometric+xray&gs_l=serp.3...1625.2757.0.3037.5.5.0.0.0.131.593.0j5.5.0...0.0...1c.NKff9agTVWM&pbx=1&bav=on.2.or.r_gc.r_pw.&fp=5dc606993b143f4d&biw=1024&bih=605](#)

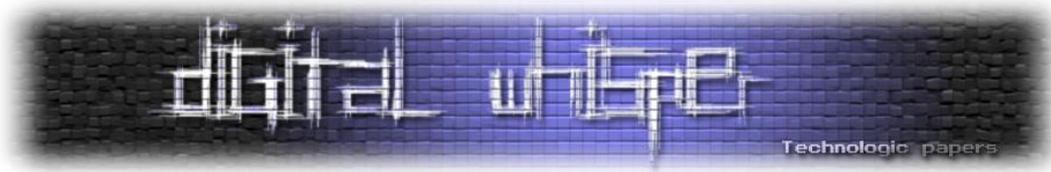
- https://www.google.co.il/search?q=xray&hl=iw&client=firefox-a&hs=w4T&rls=org.mozilla:he:official&prmd=imvnsza&source=lnms&tbn=isch&sa=X&ei=a405UNrtDqK-0QWB-ICyDg&ved=0CAoQ_AUoAQ&biw=1024&bih=605&sei=bY05UPbWEIwd0AX5hIG4Bw
- http://www.mypacs.net/repos/mpv3_repo/static/m/Home/
- <http://www.radiologyeducation.com/>
- https://www.google.co.il/search?hl=iw&client=firefox-a&hs=8y9&sa=X&rls=org.mozilla:he:official&tbs=simg:CAESYRpfCxCo1NgEGgllBgwLELCMPwgaOAo2CAESEOkF7gWKBawEiQXABKkErQoalNGbCFuZkaSX4wpslbtokP0Zzs9QOhZx9k6i42NI5BVDAsQjq7-CBoKcggIARIEN8zmSQw&tbn=isch&ei=CZY5UIGoBMXV0QXZgYH4Bw&ved=0CDAQsw4&biw=1024&bih=605&sei=C5Y5UO2cKYST0QXYkIDwDg#hl=iw&client=firefox-a&hs=sjp&rls=org.mozilla:he%3Aofficial&tbn=isch&sa=1&q=%D7%A9%D7%99%D7%A7%D7%95%D7%9D+%D7%A9%D7%99%D7%A0%D7%99%D7%99%D7%9D&oq=%D7%A9%D7%99%D7%A7%D7%95%D7%9D+%D7%A9%D7%99%D7%A0%D7%99%D7%99%D7%9D&gs_l=img.3..0i24|3.33929.36190.0.36417.12.9.0.3.3.0.147.1141.0j9.9.0...0.0...1c.HQewzYOz62U&pbx=1&bav=on.2.or.r_gc.r_pw.r_qf.&fp=4a773332d9793f81&biw=1024&bih=605

זיהוי ושכפול מפתחות על ידי צילום:

- <http://www.local.co.il/hadera/94060/article.htm>
- <http://securitylabs.websense.com/content/Blogs/3313.aspx>
- <http://cseweb.ucsd.edu/~savage/papers/CCS08OptDecode.pdf>
- <http://itp.nyu.edu/RepresentingEarth/?cat=4>
- https://www.youtube.com/watch?v=u3gGnsvOhr8&feature=player_embedded

ביומטריה קולית ממרחק בעזרת לייזר:

- <http://hot.ee.nuhk/laser.html>
- <http://www.espionage-store.com/sneak.html>
- <http://www.electromax.com/laser.html>
- <http://www.nuance.com/for-business/by-solution/customer-service-solutions/solutions-services/inbound-solutions/voice-authentication-biometrics/index.htm>
- <http://www.diy-life.com/2007/08/22/diy-laser-long-distance-listening-device/>



קריאת טביעות אצבעות ממרחק 6 מטר:

- <http://www.idairco.com/company-view>
- <http://voices.yahoo.com/startup-invents-reader-identify-fingerprints-11506442.html>
- http://blog.al.com/breaking/2012/06/idairs_new_fingerprint_reader.html
- <http://www.aos-inc.com/index.php/products/bio-prod?id=143>

אינטרנט לא חברותי

נכתב ע"י עו"ד יהונתן קלינגר

הקדמה

לפני בערך שבע שנים [ניסחתי מניפסט הקורא לאינטרנט אלחוטי בחינם כשירות ציבורי](#); הסברתי את דעתי כי צריך לחייב את הממשלה לספק אינטרנט אלחוטי חינם לציבור, ולאפשר קיום בכבוד על ידי הפחתת עלויות, שיפור התשתיות ושיתוף. מאז ועד היום קרו הרבה דברים: קודם כל, מחירי הרשת ירדו בצורה משמעותית בגלל התחרות בשוק ורפורמות בשוק התקשורת. היום, אינטרנט ביתי (ספק ותשתית) עולה פחות ממאה שקלים בחודש, ומגיע בקצבים יותר מסבירים. שנית, הפתחות הרשתות הסלולריות גרמה לכך שיותר ויותר אנשים יהיו מחוברים לרשת באמצעות הטלפונים הסלולריים שלהם. אך, במקביל, קרו כמה בעיות: הראשונה היא [שחרור תוכנות כגון Firesheep](#) שגרמה לאדם הפשוט להבין כמה הוא חשוף, והשניה היא התפתחות של שירותים כמו [WeFiFon](#), והאינטרנט החברתי של בזק, שמאפשרים שיתוף של החיבור הביתי.

בטקסט הקצר הזה, אני רוצה לדון בסכנות ובעיות בשיתוף הרשת הביתית, ולהסביר מדוע דעתי לא השתנתה, אבל עדיין צריך למצוא פתרון טכנולוגי טוב יותר.

על מה כל הרעש?

קודם, נדון בנושא של FireSheep, [שנדון לעומק כבר על ידי](#): כאשר אנחנו גולשים בחיבור אינטרנט אלחוטי שאינו מוצפן קורה משהו מיוחד: כל מי שמחובר לרשת יכול להתחבר ולראות בדיוק מה אנחנו מעבירים (עם חריגים קטנים, לא רלוונטי כרגע אבל), לאן אנחנו גולשים ואפילו לבצע התקפת [Man In The Middle](#) ולהעתיק את כל התעבורה שלנו. הדבר אומר שאם אני מתחבר באמצעות אחד השירותים החברתיים לרשת אלחוטית פתוחה, הרי שבאותו המקרה אני לא מצפין את המידע שלי, וכל אחד יכול לקרוא אותו. כלומר, אם נדבר לרגע על האינטרנט החברתי של בזק (למרות שהוא רק דוגמא, כי גם בחיבור אינטרנט במלונות יש בדיוק את אותה הבעיה): נניח שהתחברתי, הכנסתי את שם המשתמש והססמא שלי כדי לאמת את הזהות שלי, ואני גולש לנוחתי. מאותו רגע, כל מי שיתחבר לרשת (גם אם הוא לא יצליח לתת שם משתמש וססמא, אלא רק להתחבר אליה) יוכל לדעת מי אני, לאן אני גולש ואפילו לחטוף את ה-Cookies שלי ולהזדהות בשמי מול אתרים אחרים.

כלומר, השימוש ברשתות לא מאובטחות הוא מאוד בעייתי למשתמש הקצה: יש סכנות של פרטיות (כל אחד יכול לדעת לאן אתה גולש) ושל אבטחת מידע (כל אחד יכול לדעת מי אתה ואיך אתה מזדהה). זה הסוג הראשון של הבעיות; המינוי אולי פחות, אבל הסביר יותר. וזה הסוג שימנע מאנשים להשתמש בשירותי אינטרנט חברתי למיניהם.

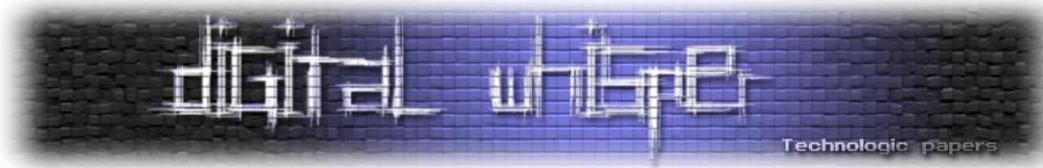
הסוגיה השנייה, הבעייתית יותר, היא של הלקוח שבחר לשתף את האינטרנט שלו. הדוגמא היא, שוב, של בזק, אבל היא לא רלוונטית אלא רק הדגמה. בזק [טוענת](#) כי החיבור באמצעות שם משתמש וסומא מאפשר לזהות את מי שהשתמש בשירות, אם היה שימוש לרעה כיוון שהמידע נאגר בשרתיה של בזק; אבל הדבר לא ברור ולא מצאתי דוקומנטציה מלאה של השימוש. אבל: נניח שאדם משתף את הרשת האלחוטית שלו, הרי שכל מי שמתחבר יכול להשתמש בה כדי לעשות פלאים לא חוקיים: החל מהורדה של חומר פדופילי, דרך שיתוף קבצים לא חוקי והרצת מניות, ועד פרסום טוקבקים בבלוגים שיהיו לשון הרע. אם יתקבל [תזכיר חוק חשיפת גולשים](#) שמאפשר לזהות גולשים אנונימיים, הרי שמה שיקרה כאן הוא מאוד בעייתי: דמינו שאדם יקבל תביעה על סמך כתובת ה-IP שלו, וזאת כאשר הוא השאיר את הרשת שלו פתוחה למשתמשים.

אגב, במשפט הפלילי קיים כבר חוק נתוני תקשורת ([חוק סדר הדין הפלילי \(סמכויות אכיפה - נתוני תקשורת\)](#)) שמאפשר למשטרה ולעוד שורה של רשויות לקבל את המידע הזה, על זהות המשתמש. על סמך חוקים דומים, היו כבר טעויות בעבר בחו"ל. לדוגמא, בשנת 2011 [אדם שהשאיר את הרשת האלחוטית שלו פתוחה נחשד בהורדת פורנוגרפיית קטינים](#); רק לאחר בדיקה פורנזית מעמיקה של המחשב שלו, התגלה שהוא דובר אמת, והדבר מעולם לא קרה.

זו, כמובן, לא אנקדוטה. גם בישראל היה סיפור דומה: בעניין עא 1806-09 [רבקה פלח \(בייבי פלוס\) נ' שירותי בריאות כללית](#) נדונה השאלה האם ראוי לחשוף גולש אנונימי. אותו מקרה קדם להחלטת בית המשפט העליון בעניין רמי מור שקבעה כי אין דרך חוקית לחשוף גולש (רעא 4447/07 [רמי מור נ' ברק אינטרנט](#)). אבל, שם קרה משהו מעניין: כתובת ה-IP אותה ביקשו לחשוף היתה שייכת לשירותי בריאות כללית; זו, מצדה, הסבירה לבית המשפט כי אין לה רישום של מי התחבר לרשת שלה. בית המשפט לא ממש היה קשוב, והורה לה לחשוף את המידע בכל מקרה. כך גם עשוי לקרות היום, במכשירי אינטרנט חברתיים.

אבל האחריות של מי שמפעיל את הרשת היא בעייתית: לדוגמא, בגרמניה בשנת 2010 [התקבלה החלטה שבצורה אפקטיבית אוסרת על שימוש ברשתות פתוחות בדיוק בשביל הסיבה הזו: לזהות את כל מי שהתחבר](#). כלומר, השיטה הגרמנית היא שאם אי אפשר לזהות, אסור להתחבר בכלל לרשת.

שתי הבעיות המקבילות כאן: של העדר הפרטיות ושל הסכנות למפעיל הרשת ידועות לכל הצדדים, ולמרות זאת הם ממשיכים להפעיל רשתות. לכן, השאלה המעניינת היא מדוע אנשים ממשיכים להשתמש בהסדר הלא יעיל הזה ולא מחפשים פתרון טוב יותר, ומעבר לזה: מדוע חברות מסחריות כמו בזק או Fon



(שעכשיו טוענת שבזק העתיקה ממנה) ממשיכות לרכב על זה ולא מזהירות את גולשיהן מהסכנות? הפתרון לשאלה כזו אינו חד-משמעי, אבל נובע מהעדפה של נוחיות על גבי פרטיות, והיא בעיה שאנו חיים עמה כל היום.

חוק המספרים הגדולים

את המונח [Shoulder Surfing](#) לא צריך להסביר. מדובר על התנהגות שבה אדם אחד מציץ למסך של חברו שנמצא בקרבתו, וזאת רק כיוון שאותו אדם אינו מאבטח את מסך המחשב שלו בצורה ראויה והמסך בוחק מספיק. כולנו מודעים לבעיה הזו ולכן גם כולנו מכירים את תסמין "הפרחה ברכבת" שמדברת על הסודות האישיים ביותר שלה בטלפון הסלולרי בקולי קולות. כולנו יודעים שאם אנחנו עושים משהו במרחב ציבורי, אין לנו ממש יכולת לשלוט על מה שאחרים מגלים, אבל אנחנו עדיין עושים את זה. לכן, לעיתים תמצאו בבתי קפה פגישות סתרים, אנשים שעובדים על פרויקטים מסווגים או מאובטחים, בגידות של בני זוג ועוד. ההנחה שלנו היא שאף אחד לא מחפש מידע, ולכן הוא לא מעניין.

מה שאנחנו לא יודעים (או רוב האנשים לא יודעים) זה שהיכולת לכרות מידע קיימת. כלומר, לאף אחד באמת אין רצון להכנס לחשבון ה-Facebook שלך. זה לא מעניין אף אחד איפה אחיך נפש בסוף השבוע, ואיפה האקסית מהתיכון מבלה היום; אבל: בקבוצה גדולה יחסית זה כן מעניין, כי המידע המצטבר מאפשר לבצע פעולות רבות. אנשים לא מניחים שאפשר לצבור כך את המידע שאפשר להשתמש בו, ולכן הם מתעלמים. בדרך כלל, כאשר אני מציג לאנשים את הסכנות בגלישה ברשת לא מאובטחת, הם אומרים לי "אז מה יש לי כבר לפחד מזה?" כאילו אין להם מידע פרטי.

מנגד, בעלי בתי הקפה שמשאירים רשתות פתוחות (או בכלל עסקים, מקומות בילוי, לימודים וכדומה) אינם מודעים לסיכונים המשמעותיים: רובם אינם מבינים שאפשר בקלות יחסית לנסות להטיל עליהם אחריות על שיתוף קבצים שנעשה במסגרת המתחם שלהם, או יותר מזה: שיכול להיות שפעילות לא חוקית שמבוצעת מאצלם תוביל לפגיעה בפרטיות של כל הגולשים שם.

יש פתרון?

עכשיו, איך פותרים את בעיית המודעות הזו, כאשר מנגד יש קמפיין של 'רשת חברתית' שמעודד שימוש ברשתות לא מוצפנות? הרי הפתרון של "לפרוץ כדי להוכיח" הוא לא חוקי ולא יעיל; לא תמיד אדם יודע שהחשבון שלו נפרץ. הפתרון צריך להיות גמול למי שמאבטח את הרשת שלו, ומייצר ענישה חלקית לרשתות לא מאובטחות. בתיאוריה, הפתרון עבורי, בתור אזרח, היא [להתחבר הביתה באמצעות SSH](#) [כאשר אני מגיע לרשת לא מאובטחת](#), ואת המשך החיבור לעשות דרך הבית. הסיבה לכך? חיבור כזה

אינטרנט לא חברותי

www.DigitalWhisper.co.il

מאבטח את התקשורת ומונע ממי שיושב לידי להאזין לי. החסרון? כמובן, שאם אתה יודע להגדיר פרוקסי בבית, אתה כנראה לא צריך לקרוא את המאמר הזה. פתרון נוסף הוא להשתמש בתוסף הדפדפן [HTTPS Everywhere](https://www.everywhere.com/) שמכריח חלק ניכר מהאתרים הגדולים לעבוד בצורה מאובטחת. אבל עדיין: לא מדובר על פתרון מושלם. מעבר לזה? אין הרבה דרכים לשמור על עצמך.

הפתרון בצד השני, של בתי הקפה שנותנים אינטרנט בחינם, הוא להרים Firewall עצמתי ובעייתי, שיחסום כל תעבורה שהיא לא סטנדרטית. כלומר, לפגוע ביכולת של הלקוחות לבצע פעילות של שיתוף קבצים, התחברות לשירותי FTP או P2P, הורדות מאסיביות שמפרות זכויות יוצרים. הבעיה היא, שגם פתרון כזה הוא לא הרמטי: הוא לא מונע ממני לכתוב תגובה מבישה באתר חדשות שמוציאה לשון הרע, או פוגעת בפרטיות, והוא לא מונע בצורה הרמטית את האפשרות שמישהו יוריד חומר פורנוגרפי מהרשת. לכן, גם שימוש כזה הוא בעייתי.

פתרון אחר הוא להפעיל שירות מעקב, שפותר אולי את הבעיה הראשונה (של שימוש לרעה ללא אחריות) אבל מגדיל את החשיפה לבעיה השנייה (פגיעה בפרטיות): כלומר, אם בית קפה מסוים יעקוב אחר כל הגולשים שלו, וישמור מידע כמו כתובת MAC (הכתובת הפיסית של כרטיס הרשת), מידע מזהה אחר כמו שם המשתמש בפייסבוק וכדומה, זה ירתיע אנשים מלעשות שימוש לא ראוי, אבל זה גם ירתיע אנשים מלהשתמש ברשת, בהתחשב בכך שהמידע הזה נשמר.

כלומר, אין ממש דרך הרמטית להגן על רשת אלחוטית בכל אחד מהצדדים, ומדובר על הסכם של אמון: אותו הסכם של אמון שנובע מכך שכשלקוח מגיע למסעדה ומזמין מזון, לא מבקשים ממנו לשלם מראש. מניחים שאם הוא הגיע, התיישב והזמין, אז יש לו את הכסף. ההנחה הזו בעייתית: היא בעייתית כי הנזק מאי תשלום חשבון (שיכול להגיע לכמה מאות בודדים של שקלים, במקרה הרע ביותר) אינו מתקרב בסדרי גודל לנזק האפשרי שיכול להגרם משימוש לרעה ברשת האלחוטית.

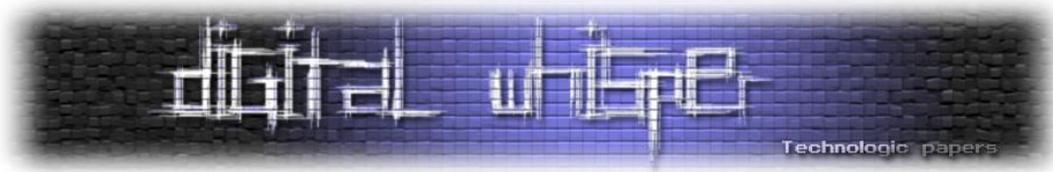
האמון הזה מבוסס על פיסות מידע שאנחנו חושבים שיש לנו: אדם שמשלם בכרטיס אשראי מותיר אחריו פיסת מידע קטנה של זהות, כך גם מצלמות 'אבטחה' שמותקנות באותו בית קפה. אבל מה קורה כשהאדם כלל לא מגיע לבית הקפה, אלא יושב בדירה למעלה ומשתמש בחיבור האינטרנט של בית הקפה כדי לצרוך תכנים לא חוקיים או פורנוגרפיה קשה? האם במצב כזה בית הקפה חי מאותו אמון? אני בספק.

לסיכום

הפתרון צריך להיות אחר: או להגדיר נקודות חיבור כאלה כ'ערי מקלט', כמו אתרי תוכן גולשים, או לסגור אותן לגמרי. הגדרה כערי מקלט משמעה כי כל תחנה שתסומן כתחנת אינטרנט פתוחה לא תהיה אחראית לשימושים שנעשים בה בדיוק כמו שאתר כמו [תפוז](#) אינו אחראי לתוכן בפורומים. במצב כזה, יחסכו מראש ההליכים המשפטיים, אבל העולם ידע שכל נזק שיגרם משם עשוי להשאר ללא סממן.

אבל זה בדיוק כמו בעולם האמיתי: גם בעולם האמיתי יש מקרים שלא מותירים ראיות, שלא ניתנים לפענוח. האקר תמיד יכול לקפוץ דרך חמישה או שישה מחשבים בדרך ולא להתגלות (ומה לעשות, ההצגה בסרטים הוליוודים של הדרך בה מזהים אותו אינה ממש נכונה).

וזו בדיוק הבעיה שצריך לטפל בה: עד עכשיו יש לנו לא מעט אנשים שמנצלים לרעה: גם אם הם עומדים בצד ואף אחד לא מכיר אותם; הבעיה היא שכשנותנים אינטרנט חברתי, או שכשמשתפים את הרשת, אף אחד לא יודע בדיוק מה קורה שם. את הסכנות האלה אנשים שוכחים, ואומרים "מה כבר יקרה לי". ואם לא יהיו אנשים שיזכירו להם את הסכנות, אנחנו נשאר בבעיה.



דברי סיום

בזאת אנחנו סוגרים את הגליון ה-35 של Digital Whisper. אנו מאוד מקווים כי נהנתם מהגליון והכי חשוב- למדתם ממנו. כמו בגליונות הקודמים, גם הפעם הושקעו הרבה מחשבה, יצירתיות, עבודה קשה ושעות שינה אבודות כדי להביא לכם את הגליון.

אנחנו מחפשים כתבים, מאיירים, עורכים (או בעצם - כל יצור חי עם טמפרטורת גוף בסביבת ה-37 שיש לו קצת זמן פנוי [אנו מוכנים להתפשר גם על חום גוף 36.5]) ואנשים המעוניינים לעזור ולתרום לגליונות הבאים. אם אתם רוצים לעזור לנו ולהשתתף במגזין Digital Whisper - צרו קשר!

ניתן לשלוח כתבות וכל פניה אחרת דרך עמוד "צור קשר" באתר שלנו, או לשלוח אותן לדואר האלקטרוני שלנו, בכתובת editor@digitalwhisper.co.il.

על מנת לקרוא גליונות נוספים, ליצור עימנו קשר ולהצטרף לקהילה שלנו, אנא בקרו באתר המגזין:

www.DigitalWhisper.co.il

"Talkin' bout a revolution sounds like a whisper"

הגליון הבא ייצא ביום האחרון של חודש ספטמבר.

אפיק קסטיאל,

ניר אדר,

01.09.2012