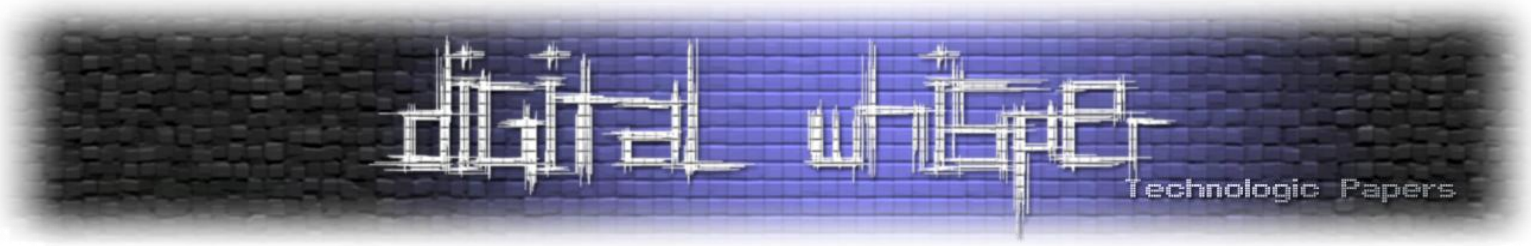


סקירת טכנולוגיות ההצפנה EFS ו- BitLocker

מאת בנימין כהן

הקדמה

הצפנה הינה רצף פעולות מתמטיות הפועלות על מידע נתון והופכות אותו להיות בלתי קריא או בלתי מובן עבור מי שלא ידע איך לפענח את ההצפנה. ישנם שני סוגי הצפנות :

1. הצפנה סימטרית.
2. הצפנה אסימטרית.

הצפנה סימטרית הינה הצפנה הכוללת מפתח (או cipher – צופן). אלגוריתם ההצפנה, הידוע לשני הצדדים (השולח והמקבל) עושה שימוש במפתח לשם הצפנה ופענוח.

אלגוריתמי ההצפנה הסימטרית מתחלקים לשני סוגים :

- Stream Cipher: אלגוריתם המצפין את כל המידע, ביט (Bit) אחר ביט עם מידע פסאודו-רנדומלי (מידע הנראה אקראי, אך בעצם אינו כזה), בדרך כלל ע"י פעולת XOR.
- Block Cipher: אלגוריתם המצפין בלוקים של מידע (בלוק אחד - 128Bit). לאלגוריתם זה מספר תצורות עבודה.
  אלגוריתמים נפוצים לסוג הצפנה זה : RC4, RC5, DES, 3DES, AES

הצפנה אסימטרית (או Public Key) תלויה בשני מפתחות אשר יש ביניהם קשר מתמטי: מפתח ציבורי ומפתח פרטי. המפתח הפרטי נשמר במקום סודי (כדוגמת SmartCard) והמפתח הציבורי ניתן לפרסום. בשונה מהצפנה סימטרית, כאן אי אפשר להצפין ולפענח באמצעות מפתח אחד. הצפנה אסימטרית נחשבת כהצפנה חזקה יותר מהצפנה סימטרית מכיוון שיש שימוש במפתחות הצפנה גדולים יותר.

בהצפנה סימטרית משתמשים במפתח באורך BIT 128-256 בעוד שבהצפנה אסימטרית משתמשים במפתח באורך BIT 1024-2048 (ויש גם מפתחות ארוכים יותר). ככל שמפתח ארוך יותר, כך קשה יותר לפרוץ את המידע המוצפן.

שימושים להצפנה אסימטרית :

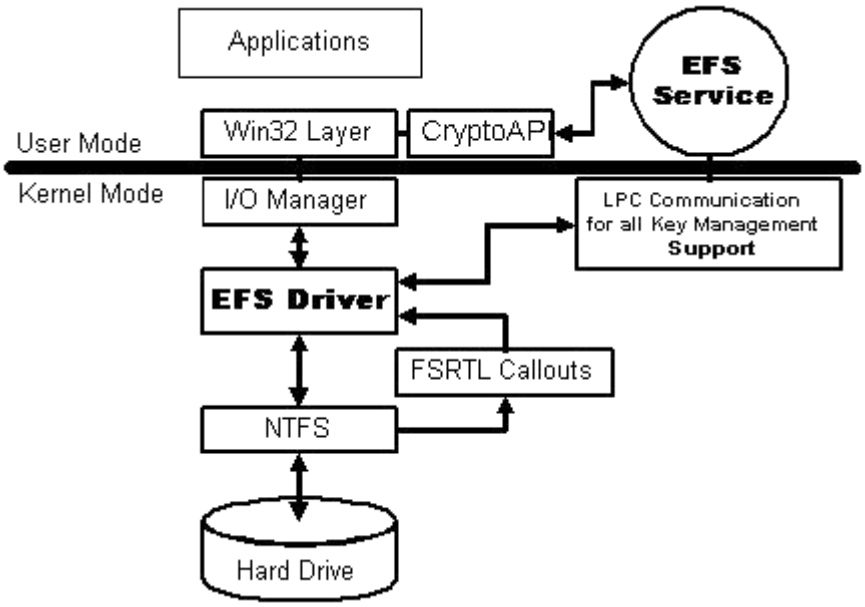
1. החלפת מפתחות סימטריים בין הצד השולח לצד המקבל.
2. חתימה דיגיטלית.

הצפנה סימטרית נחשבת להצפנה מהירה יותר מאסימטרית.

איזו הצפנה חזקה יותר? נכון להיום, חוזק הצפנה של מפתח סימטרי 128Bit שווה ערך לחוזק הצפנה של מפתח אסימטרי 1024Bit. הצפנות אלו חלשות היום ומומלץ להשתמש בהצפנות מפתח סימטרי בגודל 256Bit או אסימטרי בגודל 2048Bit.

Encrypting File System - EFS

EFS הינו רכיב של מערכת הקבצים (Ntfs). הוא מוכל בכל הגרסאות של Windows, ושימושו התחיל מ-Windows 2000 והמשיך לגרסאות הבאות. לא נדרש ידע מתקדם על מנת להשתמש ב-EFS , אך עם זאת, שימוש ב-EFS ללא הכרת השיטות המומלצות לשימוש בו עלול לתת תחושה מוטעית בכך שהקבצים אינם מוצפנים בצורה שנראה שהם. הצפנת EFS אינה מתרחשת ברמת היישום, אלא על תיקיה ברמת המערכת. אם תיקיה מסומנת על הצפנה, הקבצים אשר נוצרו בתיקיה, או שיעברו לתיקיה יהיו מוצפנים. אם משתמש מנסה לפתוח תיקיה זו, והוא בעל המפתח – היא תפתח ללא כל בעיה. במידה והוא לא בעל המפתח, הוא יקבל הודעת שגיאה "הגישה נדחתה". הצפנת קבצים זו משתמשת במפתח סימטרי.



(מקור: http://www.securityfocus.com/unix/linux/images/dicf-efs-arch.jpg)

מפתחות ה-EFS מוגנים על ידי סיסמתו של המשתמש, ובמידה והתבצעה התחברות למערכת באמצעות שם משתמש והסיסמה, המפתח נמצא אצל המשתמש, והוא יוכל להיכנס לתיקיות המוצפנות ללא כל בעיה.

EFS משתמש במפתח הצפנה סימטרי בשיתוף עם טכנולוגיית המפתח הציבורי על מנת להגן על הקבצים. קובץ הנתונים מוצפן עם אלגוריתם סימטרי (DESX). כברירת מחדל, EFS משתמש באלגוריתם DESX עם אורך מפתח של 128Bit. יש אפשרות במערכת להגדיר את השימוש באלגוריתם 3DES חזק יותר ומשתמש עם אורך מפתח של 168Bit. בעורך ה-Registry מבצעים את השינויים האם להשתמש באלגוריתם DESX או באלגוריתם 3DES.

המפתח משתמש בהצפנה סימטרית שנקראת FEK (File Encryption Key), FEK מאוחסן בקובץ, יחד עם המפתח הציבורי שמשתמש באלגוריתם RSA. הסיבה לכך שיש שימוש בשני האלגוריתמים היא מהירות ההצפנה.

תהליך ההצפנה

- צעד ראשון אחרי ההצפנה, NTFS יוצר קובץ LOG שנקרא Efs0.log כקובץ מוצפן. ה-EFS דורש גישה ל-CryptoAPI context והוא עושה זאת בעזרת Microsoft Base Cryptographic.
- ברגע שנפתח ה-Crypto context הוא יוצר FEK. אחרי שיצרנו את ה-FEK אנחנו צריכים גם מפתח ציבורי. במידה ולא קיים מפתח ציבורי (בד"כ מדובר בהפעלה ראשונה של המערכת), EFS מייצר מפתח ציבורי חדש. הוא משתמש במפתח באורך 1024Bit עם אלגוריתם RSA ומצפין אותו ביחד עם ה-FEK. לאחר שיש לנו מפתח פרטי (FEK) ומפתח ציבורי- EFS יוצר DDF (Data Decryption Field) למשתמש הנוכחי, ומאחסן בו את ה-FEK שלו ואת המפתח הציבורי.
- בנוסף, EFS יוצר DRF ומאחסן שם את ה-FEK ואת המפתח הציבורי של ה-RECOVER. DRA נוצר בנפרד לכל סוכן Recovery. לאחר שהקובץ הוצפן, רק למשתמשים התואמים למפתחות (הנמצאים ב-DDF או DRF) יש את האפשרות לגשת לקובץ. רק משתמש שיחזיק ב-FEK ובמפתח הציבורי יוכל להיכנס לקובץ.

תהליך השחזור

- תהליך השחזור דומה לתהליך הפענוח. נעשה שימוש ב-DRF (ולא ב- DDF) ובמפתח השחזור של הסוכן על מנת לפענח את ה-FEK.

אבטחה – פגיעות במערכת ופתרונות

שתי בעיות אבטחה משמעותיות קיימות ב-Windows 2000:

- <u>פענוח קבצים באמצעות חשבון מנהל מקומי</u>
ב-Windows 2000 המנהל המקומי (LOCAL) הינו ברירת המחדל של DRA (Data Recovery Agent). הוא מסוגל לפענח את כל הקבצים המוצפנים עם – EFS על ידי כל משתמש מקומי.

Windows 2000 לא יכול לתפקד ללא סוכן שחזור, ולכן תמיד יהיה מישהו שיוכל לפענח קבצים מוצפנים של המשתמשים. כל מי שאינו מנהל (Admin) ומצטרף למערכת, יהיה פגיע בכך שיהיה ניתן לפענח את הקבצים שלו דרך המנהל המקומי.

פתרון לבעיה: במערכת XP, ובמערכות הבאות אחריה, לא הוגדרה ברירת מחדל עבור Data Recovery Agent.

- <u>גישה למפתח הפרטי דרך איפוס סיסמא</u>
ב-Windows 2000, מפתח ה-RSA הפרטי של המשתמש אינו מאוחסן רק בצורה מוצפנת, יש גם גיבוי למפתח הפרטי RSA שמוגן בצורה חלשה. אם לתוקף יש גישה פיזית למערכת (Windows 2000), הוא יכול לאפס את הסיסמא של המשתמש, ובכך להיכנס ולהשיג גישה למפתח הפרטי בעזרתו ניתן לפענח את הקבצים. הסיבה לכך היא שהמפתח הפרטי נשמר כגיבוי במערכת, מוצפן עם LSA שאליו יכול להגיע כל מי שהתחבר למערכת בצורת – LocalSystem.

פתרון לבעיה: במערכת XP והבאות אחריה המפתח של המשתמש הפרטי RSA מגובה באמצעות מפתח ציבורי שמבצע התאמה למפתח פרטי אשר ממוקם ב-Active Directory.

סיכום EFS

- רכיב של מערכת הקבצים NTFS.
- ההצפנה מתרחשת ברמת התיקייה ולא ברמת היישום.
- ההצפנה מופעלת החל מגרסת Windows 2000 והבאות אחריה.
- שימוש בהצפנה סימטרית על מנת להצפין את המידע.
- האלגוריתם שבו נעשה שימוש כברירת מחדל הוא – DESX.
- אורך מפתח של אלגוריתם זה הינו 128Bit.
- יש אפשרות דרך ה- Registry לשנות את האלגוריתם ל-3DES אשר מצפין את המידע באורך מפתח של 168Bit.

BitLocker

BitLocker הינה תוכנה להצפנת דיסק מלאה, הכלולה במהדורות ה-Ultimate ו-Enterprise של Vista, Win7 וב-Windows Server 2008. בעזרת תוכנה זו ניתן להגן על נתונים בעזרת הצפנה. הצפנה באמצעות תוכנה זו היא אחת הדרכים הטובות להגן על מחשבים ניידים מפני אובדן נתונים כאשר המחשב נגנב או אובד.

BitLocker דורשת אבטחה על ההצפנה שהתוכנה משתמשת אך קיימת בעיה: האלגוריתמים שקיימים כיום, העונים על דרישות האבטחה איטיים מדי, ולכן אינם מתאימים. ואילו, לא ניתן להשתמש באלגוריתם חדש, לפני שנחקר במשך מספר שנים, ושנכתבה עליו ביקורת ציבורית.

הבעיה נפתרה באמצעות שילוב של אלגוריתם AES בשילוב עם CBC עם מרכיב חדש שמכונה – Diffuser. שכבת ה-Diffuser מוסיפה מאפייני אבטחה נוספים הרצויים בהגדרות ההצפנה, אך לא ניתנים ע"י שיטות ההצפנה של AES-CBC.

על ידי שילוב של AES-CBC ו-Diffuser אנו נהנים משילוב של שני עולמות לאבטחת הנתונים: מחד - אנו יכולים להשתמש בכל מאפייני האבטחה המסופקים לנו ע"י אלגוריתמי ההצפנה AES-CBC, ומאידך - אנו יכולים לעשות שימוש במאפייני אבטחה נוספים שלא יסופקו ע"י שימוש ב-AES-CBC בלבד, במהירות העולה על האלטרנטיבות המצויות כיום.

BitLocker תומכת במפתחות הצפנה באורך של 128Bit ו – 256Bit עם או בלי Diffuser. הגדרת ברירת המחדל הינה שימוש באלגוריתם AES-CBC , במפתח הצפנה באורך של 128Bit עם Diffuser. בכל מקרה, הגדרות אלו ניתן לשנות בעזרת ה-Local Group Policy Editor.

קיימות 3 אופציות (מנגנוני אימות) לשימוש עם ה-BitLocker:

1. מפתח USB– על המשתמש להוסיף מכשיר USB שבו נמצא המפתח להפעלת המערכת המוגנת. שימוש ב-USB דורש שה-BIOS יכיר בקריאה מהתקן USB.
2. שימוש ב-TPM 1.2(Trusted Platform Module (TPM – במצב זה יש להשתמש בחומרת ה-TPM על מנת לשמור את המפתח של ההצפנה, כאשר מפתח ההצפנה מוצפן על ידי שבב ה-TPM. רק כאשר מחברים את ה-TPM והוא מזהה את המפתח ניתן להיכנס למערכת.
3. אימות פרטי – מצב זה מחייב את המשתמש לספק אימות לפני האתחול בצורת קוד PIN.

הצפנת קבצים זו משתמשת במפתח סימטרי.

*TPM- Trusted Platform Module הוא שבב אלקטרוני התומך בתכונות אבטחה מתקדמות כדי להצפין את כונן מערכת ההפעלה.זה המקום שבו ה-BitLocker מאחסן את מפתח ההצפנה.

אבטחה – אפשרויות שונות לפגיעה במערכת.

בתאריך 10.12.09 התפרסמה ידיעה בנושא אבטחת המערכת של BitLocker. חוקרי המכון Fraunhofer SIT הגרמני הודיעו כי הצליחו למצוא מספר שיטות לפריצת מנגנון האבטחה של BitLocker. כל הפריצות שתוארו היו קשורות בהתערבות אנושית על המחשב ובטעויות של המשתמש אשר הוכיחו שוב, כי ה"חוליה החלשה" בתחום אבטחת המידע נעוצה בנו - המשתמשים.

במסמך המפרט את המחקר הובאו מספר שיטות לשבירת מנגנון ההצפנה. בכל אחת מהשיטות קיימת התערבות של בעל המחשב, או מישהו בעל הרשאות Admin אשר יקיש את קוד ה-PIN על מנת לפתוח את מנגנון ההצפנה. שיטה אחת מתארת את הצורך להתחבר פיזית למחשב, ולשתול בו קובץ (מנגנון הזדהות מזוייף) ל-BitLocker. שיטה נוספת מדברת על האפשרות להתעסק עם רכיב החומרה TPM יחד עם השתלת רכיב האזנה (Sniffing) על המערכת. באמצעות פעולה זו מנגנון ההצפנה ייחסם ויצטרכו לעשות Recovery אשר במהלכו יוכנס הקוד מנהל וכך ה-Sniffing יקלוט את הקוד ויעביר אותו ברשת בצורה מרוחקת לפורץ.

סרטון המתאר הדגמה חלקית של שיטות הפריצה:

http://testlab.sit.fraunhofer.de/content/output/project_results/bitlocker_skimming/bitlockervideo.php?s=2

הנקודה החשובה בעניין, היא שכל הפריצות המתוארות כאן דורשות התערבות פיזית של מנהל המחשב שיצטרך להכניס את קוד ה-PIN או קוד ה-RECOVERY על מנת שהפורץ יוכל לקלוט את הקוד - ולהשתמש בו לאחר מכן להשגת המידע הרצוי.

פתרון לבעיה: הדרך היחידה להתמודד עם "החוליה החלשה" (המשתמשים), היא הסבר לכלל המשתמשים על חשיבות השימוש בתוכנה, ועל חשיבות המידע הרגיש הנמצא, ועל תהליכי עבודה תקינים ומסודרים - אשר יגרמו בסופו של דבר לעליה מסיימת ברמת האבטחה ברמת המשתמש, ובכך, למנוע פגיעות אשר יכולות להיגרם כתוצאה משימוש לא "חכם" במערכת.

בנוסף, ישנה חברה בשם Passware, המאפשרת לכל המעוניין את פריצת ה- BitLocker. מה הכוונה? חברת Passware הינה חברה המייצרת תוכנות לפענוח הצפנות ושחזור סיסמאות של תוכנות נפוצות להצפנה. לאחרונה השיקה החברה את מוצר הדגל שלה- Passware Kit Forencsic 9.5. Passware Kit Forencsic 9.5 היא התוכנה המסחרית הראשונה אשר יכולה לזהות מפתחות הצפנה בכוננים שהוצפנו באמצעות ה-BitLocker, ויכולה לפענח את המידע הנמצא בתוכם. עלותה נאמדת ב- 800$. תוכנה זו מסוגלת לסרוק כל כונן קשיח, לזהות את סוגי הקבצים המוצפנים הנמצאים עליו, ולפענח את ההגנות שלהם, על ידי שימוש באלגוריתמים מתקדמים לפענוח ושחזור מידע. ישנה גרסה ניידת של התוכנה הפועלת מכונן USB , אשר סורקת ומשחזרת סיסמאות של קבצים מוצפנים, ללא פגיעה במחשב עליו היא מופעלת. באמצעות תוכנה זו ניתן להוציא את המידע ללא כל בעיה, ואף מבלי שבעל המחשב ידע לזהות

האם מישהו נגע והוציא מידע (בדיקת LOGS או כל תוכנה אחרת). הסיבה לכך היא בגלל שהכול מבוצע בסביבה וירטואלית.

סיכום BitLocker

- BitLocker הינה תוכנה להצפנת דיסק מלאה.
- בעזרת תוכנה זו יכול משתמש להגן על נתונים בעזרת הצפנה.
- כברירת מחדל התוכנה משתמשת באלגוריתם AES-CBC במפתח הצפנה באורך של 128Bit עם Diffuser.
- BitLocker תומכת במפתחות הצפנה באורך של 128Bit ו – 256Bit עם או בלי שכבת Diffuser.
- הגדרות אלו ניתנות לשינוי בעזרת ה - Local Group Policy Editor.
- הצפנת קבצים זו משתמשת במפתח סימטרי.

ההבדלים השונים בין הצפנת EFS להצפנת-BitLocker

BitLocker מצפין את כל הקבצים האישיים וקבצי המערכת הנמצאים בכונן של מערכת ההפעלה, בכוננים קבועים או כוננים נשלפים (USB), להבדיל מ-EFS - המצפינה קבצים ותיקיות בנפרד ואינה מצפינה את הכונן בצורה מלאה.

BitLocker אינו תלוי בחשבונות המשתמשים: BitLocker פועל או מבוטל, עבור כל המשתמשים או הקבוצות, להבדיל מ-EFS אשר מצפין קבצים בהתבסס על חשבון המשתמש המשויך אליו. כל אחד מהמשתמשים יכול להצפין את הקבצים שלו באופן עצמאי.

EFS אינו עושה שימוש ברכיב חומרה מסוים, להבדיל מ-BitLocker המשתמש ב- Trusted Platform Module (TPM) שבב מיוחד הקיים במחשבים רבים שתומך בתכונות אבטחה מתקדמות, כדי להצפין את כונן מערכת ההפעלה.

ב-BitLocker עליך להיות מנהל מערכת על מנת לגשת ולהפעיל או לבטל את ההצפנה, בעוד ב-EFS כל משתמש יכול להצפין את המידע שהוא חפץ בו.

הערה: אין מניעה להשתמש בשני סוגי ההצפנה. הצפנת EFS שומרת את מפתחות ההצפנה במחשב, כאשר הצפנת BitLocker יכולה לעזור בשמירה על מפתחות אלו באמצעות מניעת אתחול של המערכת (והפעלת המערכת בעזרת אחד מהמנגנונים שבהם BitLocker משתמש כגון TPM, USB או אימות בעזרת קוד PIN).