Digital Whisper
Technologic Papers

פיצול מידע בשירותי ענן

מאת מריוס אהרונוביץ'

הקדמה

השימוש בשירותי מחשוב בענן (cloud computing) מתרחב בשנים האחרונות באופן מהיר. השירותים מספקים יכולת גידול, דינמיות וצמצום עלויות הטמעה ותפעול IT של ארגונים. יחד עם זאת, שירותים אלו יוצרים אתגרים לא פשוטים בנושא חיסיון וזמינות המידע, כאשר ספק השירות הינו האחראי הבלעדי לניהול תשתיות המחשוב ואבטחת המידע.

קיימות דרכים רבות לשמור על חיסיון של מידע, מיישום של סטנוגרפיה (הסתרת מסרים), דרך מנגנוני הרשאות ועד להצפנות מתוחכמות. אך כל המידע נמצא שם, בצורה כזו או אחרת, במקום אחד, זמין לגורם מספיק נחוש ובעל משאבים מתאימים, כדי למצוא ולחשוף אותו.

מעבר לחיסיון המידע, גם זמינות המידע הינה קריטית במקרים רבים ופגיעה במרכז מידע, גם אם הוא נמצא בענן, יכול לגרום לאיבוד כל המידע השמור בו. למרות שקיימים שירותים בענן המכילים מספר מרכזי מידע הפזורים גיאוגרפית, הם עדיין כולם מנוהלים על ידי אותם מנגנונים. ניתן כמובן לשכפל את המידע במספר עננים ואף להצפין את המידע לפני שכפולו, אבל אז נגדיל את הסיכון לחשיפתו, למשל בגישה לא מורשית לענן אחד, על ידי שימוש בסיסמה פשוטה מידי לפתיחת ההצפנה.

הצפנת המידע יוצרת מפתחות הצפנה שיש לנהל ופה קיימת דילמה: אם מפתחות אלו יאוחסנו בשירות כלשהו בענן, אזי תאופשר גישה למידע על ידי ספק השירות, דבר המייתר כשלעצמו את הצורך בהצפנה מלכתחילה. אם מפתחות ההצפנה יושארו בתחנות משתמשי השירות, זמינות המידע תפגע במקרה של כשל מקומי.

שיטה לפיצול מידע - Secret Sharing

אז היכן כדאי לשים את מפתח ההצפנה או את המידע עצמו? אחד הפתרונות הקוסמים לאתגרים אלו הוא פיצול של המידע המוצפן במספר שירותי אחסון בענן שונים. בצורה זו ניתן לצמצם את התלות בזמינות שירות בודד בענן או בבקרות אבטחת מידע המיושמות על ידי ספק השירות.

ניתן לפצל את המידע, הסוד, באופן אקראי, בין מספר גורמים (למשל שירותי אחסון בענן), כך שאף גורם לא יוכל לחשוף את המידע ללא סיוע של האחרים. כדי לחשוף את המידע, נדרשים כולם אם חלקם,

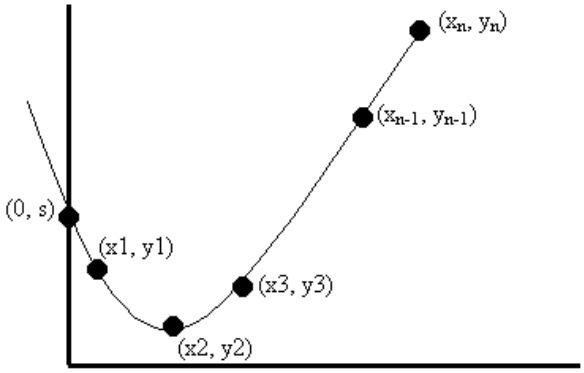
לשתף פעולה ולשלב את החלקים השונים שלהם בפונקציית שחזור. כלומר, גם אם תוקף יצליח להגיע לחלק אקראי של המידע השמור בשירות בענן אחד, הוא לא יוכל לחשוף את המידע. ניתן ורצוי גם להצפין את המידע, ולפצל גם את מפתח ההצפנה.

אחת השיטות הפשוטות ליישום נושא זה היא ביצוע פעולת XOR של המידע שאותו רוצים לשמור (נניח מספר) עם מספר אקראי, והעברת התוצאה לגורם אחד ואת המספר האקראי לגורם שני (ולא לשכוח למחוק את המקור). כדי לחשוף את המידע, שני הגורמים צריכים לבצע פעולת XOR בין שני המספרים שקיבלו. שיטה זו ניתנת להרחבה למספר גדול של גורמים, בהתאם לצורך.

שיטה מתוחכמת יותר מאפשרת שחזור של המידע תוך שילוב של קבוצה מצומצמת בלבד מתוך החלקים שחולקו. בדוגמא הקודמת, אם גורם אחד איבד את החלק שלו או לא מעוניין לחשוף אותו (כמו במקרה של פגיעה בזמינות שירות בענן אחד), לא יהיה ניתן לשחזר את המידע כלל. אך אם נצליח לפצל את המידע לארבעה גורמים שונים, ונאפשר רק לכל שניים מהם לשחזרו, נוכל ליצור יתירות בתהליך.

פרופסור עדי שמיר (אחד ממציאי אלגוריתם ה-RSA) הציע בשנת 1979 שיטה פשוטה לפיצול סודות (secret sharing) המבוססת בצורה מופשטת על גרפים. על מנת לצייר קו ישר מספיקות 2 נקודות, על מנת לצייר פרבולה מספיקות שלוש נקודות, וכן הלאה. נוכל לצייר קו מסדר כלשהו שמאפייניו אקראיים (מלבד הסוד שעליו רוצים להגן), ולחלק נקודות עליו לכל גורם שנרצה לשתף את הסוד איתו. מכיוון שכל גורם מקבל רק נקודה אחת, אין לו ידע לגבי הסוד עצמו. סדר הקו יגדיר כמה חלקים יהיה צריך לשלב ביחד על מנת לשחזר את הסוד המקורי. למשל, נוכל לצייר קו ישר עם שיפוע אקראי כשהסוד מוגדר כמפגש שלו עם ציר y. אחר כך נחלק ארבע נקודות שונות עליו לארבעה גורמים שונים, אבל רק שניים מהם, כל זוג אפשרי מתוך ארבעת הגורמים, יצטרכו לשלב את הנקודות שלהם על מנת לשחזר את הסוד.

באופן כללי אלגוריתם זה נקרא: (k,n)-threshold scheme. את הסוד מפצלים ל-n חלקים אקראיים שגודלם כגודל הסוד. שילוב של K חלקים (מספר קטן מ-n) ומעלה יכול לאפשר את שחזור הסוד. שילוב פחות מ-K חלקים לא יכול לאפשר גילוי של שום פרט על הסוד. לפיכך, איבוד של חלקים כלשהם לא פוגע בשחזור הסוד, כיוון שניתן לשלב חלקים אחרים.



[ציור 1 - פיצול של סוד למספר חלקים באמצעות גרף פרבולה]

שיטה זו מוגדרת כמאובטחת ללא תנאי (unconditionally secure), כלומר היא מאובטחת גם אם לתוקף קיימים משאבים אינסופיים. זאת מהטעם הפשוט, חסרים לו שאר החלקים בפזל שרק שילובם יאפשר את השחזור. חשיפת המידע הרגיש תדרוש פריצה לכל קבוצת k העננים שבהם שמורים חלקי הסוד.

יתרה מכך, גם אם תשתיות שירות בענן אחד נפרצו והחלק שהועבר אליו נחשף, השיטה מאפשרת יצירת סדרה חדשה של חלקי סוד וחלוקתם לעננים האחרים שלא נפרצו, ללא כל תלות בסוד עצמו או שינוי שלו ובאופן שייתר את חלק הסוד שכן נחשף. אותו חלק לא יוכל לשמש יותר לחשיפת הסוד, כיוון שקיימת סדרה חדשה של חלקים המפוצלים בעננים שונים.

שיפור יעילות פיצול המידע

החסרון היחידי בשיטת ה-secret sharing הוא היעילות הנמוכה שלה עבור פיצול של מידע רב. העברת ואחסון חלקי הסוד דורשים רוחב סרט ומקום אחסון בכמות השווה למכפלת גודל הסוד בכמות החלקים. אם מדובר בקובץ גדול, למשל, 1GB, וב-5 חלקים, אזי ידרש גודל אחסון של 5GB לאחסון כל חלקי הקובץ. לכן, שיטה זו מתאימה יותר לשימוש עם סודות קטנים (למשל מפתחות הצפנה), ופחות לשימוש עם סודות גדולים (כמו קבצים גדולים או בסיסי נתונים).

קיימת גם שיטה הנקראת "secret sharing made short" המשלבת את ה- information dispersal algorithm (IDA - שפותח על ידי פרופסור מיכאל עוזר רבין בשנת 1989) עם שיטת ה-secret sharing ומאפשרת לשפר את היעילות שלה, עבור פיצול קבצים גדולים. כל זאת על חשבון חסינות מפני שימוש במשאבים אינסופיים בצד התוקף. שיטה זו אומנם פחות מאובטחת באופן תאורטי, אך תוקף פוטנציאלי שינסה לגלות את הסוד יצטרך לחדור למספר שירותים בענן ולהתגבר גם על תהליך החלפת חלקי הסוד השונים. לפיכך, מומלץ להשתמש בשיטה חדשה זו עבור שמירת קבצים גדולים באופן מאובטח, בשל יעילותה. יחד עם זאת, מומלץ גם להגדיל את כמות שירותי האחסון בענן המשתתפים בתהליך פיצול המידע כדי לשמור על רמת אבטחה גבוהה.

סיכום

פתרונות המשלבים מנגנוני פיצול מידע (split knowlge, split key) שולבו בעבר בעיקר בהגנה על מידע רגיש בתוך ארגונים או בשמירה של מפתחות הצפנה, דוגמא לכך יכולה להיות שימוש במנגנוני dual control בגישה או ביצוע פעולות במידע רגיש בתוך רכיב HSM[1] (לנושא זה קיימות הגדרות[2], הנחיות ותקנים[3]). בשנים האחרונות נרשמו מספר פטנטים המשתמשים ב-IDA וב-secret sharing כבסיס ל-Information Assurance תוך שיפור זמינות וחיסיון המידע. כמו כן, קיימים כבר היום מספר פתרונות המיישמים אבטחת מידע בשירותי אחסון בענן בשיטה חדשה-ישנה זו, הכוללים מספר רבדים כמו הצפנת המידע ופיצול אקראי של המידע המוצפן ומפתח ההצפנה עצמו בין מספר שירותי אחסון בענן. יישומים אחרים מאפשרים היום הצפנת המידע השמור בענן ופיצול מפתח ההצפנה בלבד בין גורמים שונים. פתרונות אלו מכילים גם תשתית לניהול שינויים של החלקים השונים.

יש לזכור שכשמפתח ההצפנה בלבד מפוצל בשירותי ענן, עדיין כל המידע המוצפן שמור במקום אחד ולאחר גישה אליו, ניתן לבצע ניתוח קריפטוגרפי ולחשוף את המידע הלא מוצפן. מנגנונים לפיצול מידע רגיש בענן יכולים להשתלב בשירותי אחסון מידע, סנכרון מידע, שיתוף קבצים ומרכזי מחשוב בענן, יחד עם מגמת ה-Intercloud המאפשרת יצירת קישוריות בין שירותים בענן לצורך שיתוף משאבים.

על המחבר

מריוס אהרונוביץ' הוא ראש תחום אבטחת תקשורת בחברת אבנת אבטחת נתונים, מהנדס חשמל ומחשבים תואר שני ובעל הסמכת CISSP.

[1] Hardware Security Module

[2] https://www.ccn-cert.cni.es/publico/serieCCN-STIC401/en/s/split_knowledge.htm
https://www.ccn-cert.cni.es/publico/serieCCN-STIC401/en/s/split_key.htm

[3] https://www.pcisecuritystandards.org/documents/PCI_HSM_Security_Requirements_v2.pdf