digital whisper
Technologic Papers

תשתית מפתחות ציבוריים

מאת: עמיחי פרץ קלופשטוק

הקדמה

פעמים רבות בעולם המחשבים ואבטחת המידע, נוצר צורך ברשת תקשורת מאובטחת ומהימנה, אשר העברת נתונים דרכה תהיה סודית ובטוחה מפני שינוי - זדוני או מקרי כאחד. ישנם פתרונות רבים לבעיה זו, כשהבולטים שבהם מגיעים מתחום הקריפטוגרפיה. במאמר זה אסקור את שיטת המפתחות הפומביים, כיצד היא עובדת, מהם היתרונות והחולשות שלה, ודרכים שונות לממש אותה כתשתית תקשורת.

הצפנה סימטרית ואסימטרית

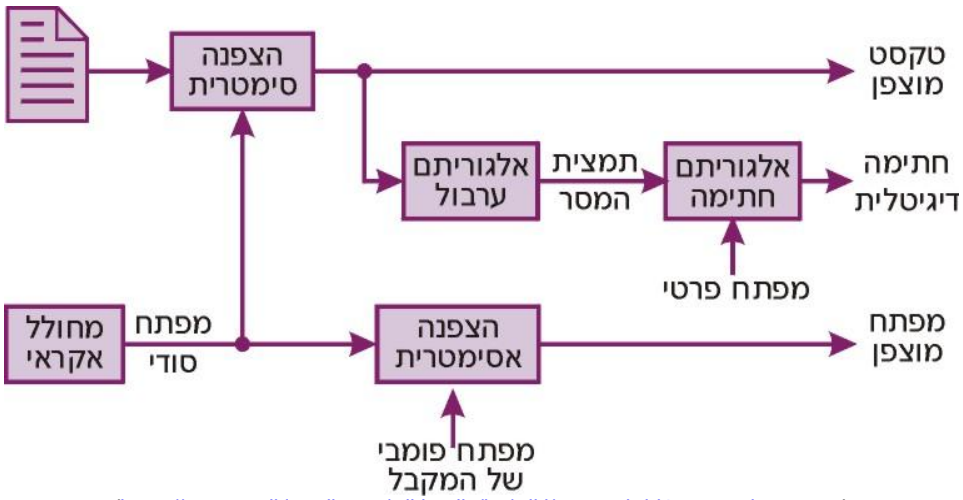
בתורת הקריפטוגרפיה, קיימות שתי צורות הצפנה עיקריות: הצפנה סימטרית, בה מפתח ההצפנה זהה למפתח הפענוח, והצפנה אסימטרית, בה קיימים זוגות של מפתחות הצפנה תואמים זה לזה. עקב התכונות המתמטיות של המפתחות האסימטריים, הודעה שתוצפן באמצעות מפתח אחד תוכל להיות מפענחת רק באמצעות המפתח השני, ולהפך.

לכל אחת מן השיטות הנ"ל יתרונות וחסרונות, אך הסיבה העיקרית שבזכותה אנו מעדיפים להשתמש בהצפנה אסימטרית לתקשורת מסוג זה, היא שבשונה מהצפנה סימטרית, בה יש צורך להעביר את מפתח ההצפנה בצורה סודית לשני הצדדים שמשתתפים בתקשורת, בהצפנה אסימטרית אין צורך לשמור על סודיות המפתחות - למעשה, ניתן לפרסם אותם באופן פומבי באינטרנט.

הצפנה מבוססת מפתח פומבי

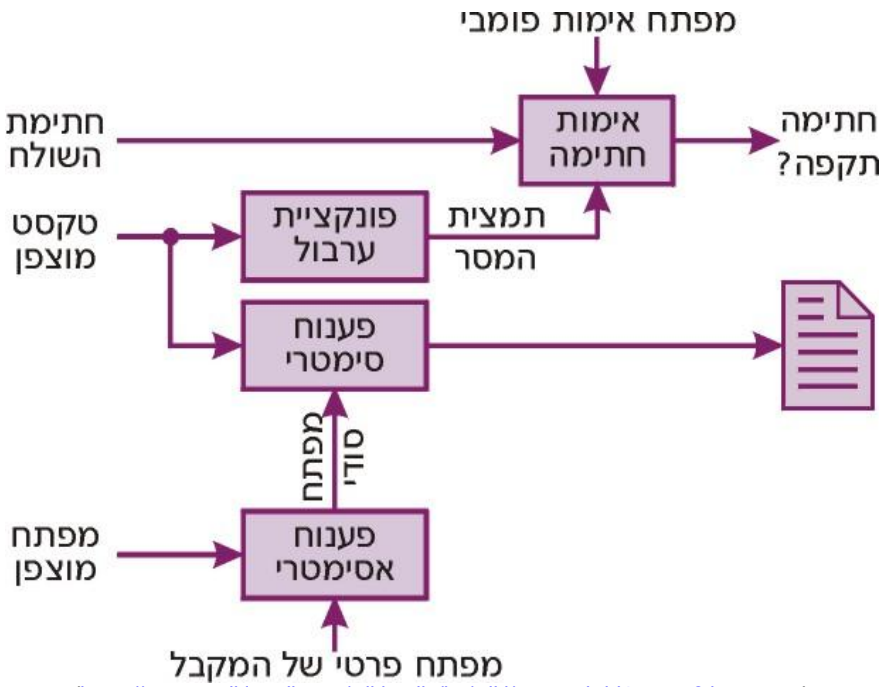
כאשר משתמשים בהצפנת מפתח פומבי, לכל גורם ברשת התקשורת ישנם שני מפתחות. באמצעות מפתח אחד, שנהוג לכנותו מפתח ציבורי או פומבי (Public Key), ניתן להצפין הודעות אל האדם, אשר רק הוא יוכל לפענח. מפתח זה מופץ באופן חופשי לכל דורש, על גבי שרתי מפתחות יעודיים או בדרכים אחרות. המפתח השני, הנו מפתח סודי, אשר רק לבעליו יש גישה אליו, ונקרא מפתח פרטי (Private Key). מפתח זה משמש את בעליו כדי לפענח הודעות שהוצפנו באמצעות המפתח הפומבי שלו, ולחתום על הודעות יוצאות.

לדוגמה, אברהם מעוניין להעביר הודעה סודית אל יצחק. ראשית אברהם יחתום על תמצית (Hash) של ההודעה המקורית, יצרף אותו אל ההודעה. כעת אברהם יצפין את כל המסר בצופן סימטרי, ואת המפתח יצפין באמצעות המפתח הציבורי של יצחק, וישלח את ההודעה המוצפנת+המפתח המוצפן אל יצחק דרך ערוץ תקשורת לא מאובטח .ניתן לראות את התהליך המלא בדוגמה הבאה:



(במקור: https://secure.wikimedia.org/wikipedia/he/wiki/קובץ:HybridSystem1.jpg)

כאשר יצחק יקבל את ההודעה, ראשית הוא יפענח אותה בעזרת המפתח הפרטי שלו. לאחר מכן, הוא יוודא שאכן ההודעה נשלחה על ידי אברהם, בכך שיפענח את התמצית המוצפנת שצורפה להודעה, וישווה אותה מול תמצית שנוצרה באותו רגע מההודעה עצמה. כל שינוי קטן בהודעה יתגלה בצורה כזו באופן מיידי. תהליך זה מוצג באיור הבא:



(במקור: https://secure.wikimedia.org/wikipedia/he/wiki/קובץ:HybridSystem2.jpg)

כך, אברהם יודע שרק יצחק יהיה מסוגל לקרוא את ההודעה, משום שרק לו יש את המפתח הפרטי הנכון, ויצחק ידע שרק אברהם יכל לשלוח לו את ההודעה, כיוון שהיא חתומה עם המפתח הפרטי שלו.

חולשה פוטנציאלית

נתאר לעצמנו מצב כזה: יצחק חי בישראל, בזמן שאברהם חי בארצות הברית. יש להניח, שהם לא ייפגשו לעתים קרובות, ויתכן שהתקשורת שלהם מבוססת על מפתחות פומביים שנשלחו בדוא"ל או הופצו דרך שרת מפתחות.

מצב כזה עשוי לפתוח דלת למתקפת האדם שבאמצע (Man in the middle). בפשטות, מדובר על מצב בו גורם זדוני כלשהו יתחזה ליצחק כלפי אברהם, ולאברהם כלפי יצחק. אם הפושע גורם ליצחק לחשוב שהמפתח הציבורי שלו הוא המפתח הציבורי של אברהם, ולאברהם לחשוב שהמפתח הציבורי שלו הוא של יצחק, כל התקשורת ביניהם תהיה נתונה לחסדיו - הוא יוכל להאזין, לסנן, לזייף ולשנות הודעות, אשר יראו אמינות לחלוטין. למעשה, חוזקה של מתקפה זו הוא בכך שאין לקרבן כל סיבה לחשוד בפעילות זדונית, ובכך שהתוקף מקבל אמינות גבוהה יחסית.

חתימה על מפתחות

ישנן שיטות רבות להתגבר על בעיה זו, וכולן מבוססות על זיהוי פיזי של האדם, שיקושר למפתח ציבורי מסוים. בצורה כזאת, לגורם זדוני יהיה קשה בהרבה להתחזות לאדם אחר.

הבעיה, כמובן, היא הצורך בזיהוי אמין - זיהוי פנים אל פנים, באופן אישי או על ידי גוף שלישי אמין. כאשר מזהים את הגורם המבוקש, חותמים על המפתח הציבורי שלו (למעשה, על תמצית של המפתח), באמצעות המפתח הפרטי של הגורם המאשר.

קיימות שתי שיטות עיקריות לזיהוי כזה:

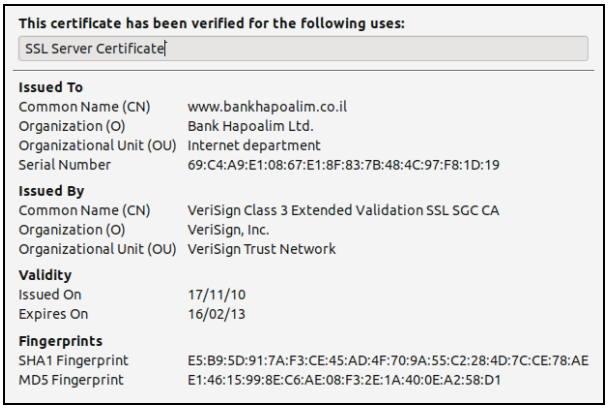
- שיטת הרשות המאשרת (Certificate Authority)
- שיטת רשת האמון(Web of trust)

<u>רשות מאשרת</u>

בשיטה זו, ישנן חברות אשר עוסקות בווידוא זהותם של גורמים, ובחתימה על מפתחותיהם. גורם אשר מבקש לקבל אישור כזה, צריך לאמת את זהותו על פי דרישות ונהלי החברה. רשויות מאשרות נפוצות בעיקר במגזר העסקי, בו יש צורך בזיהוי אמין מעל לכל ספק, ובתחום האינטרנט, לצורכי אימות של אתרים שאין באפשרות הגולשים לאמת בעצמם.

שיטה זו נפוצה לרוב באתרי אינטרנט גדולים, לצורך שימוש בפרוטוקול SSL. במקרים כאלו, האתר מאמת את זהותו באמצעות אישור אבטחה חתום על ידי רשות מאשרת, אשר המפתח הציבורי שלה מוטמע בדפדפן או מתקבל משרת מיוחד. בזכות האמון ברשות המאשרת (שנובע מגורמים רבים), ניתן לסמוך על זהותו של אתר האינטרנט.

האמון של המשתמשים הנו בחברות הללו בלבד, ואישורים הדדיים בין "משתמשים" אינם נפוצים, ואינם נחשבים לבטוחים. חברות מוכרות בתחום זה כוללות את VeriSign, Comodo, RSA, ועוד... ניתן לצפות באישורי האבטחה באמצעות הדפדפן - הנה, לדוגמה, אישור האבטחה של בנק הפועלים:



This certificate has been verified for the following uses:

SSL Server Certificate

Issued To	
Common Name (CN)	www.bankhapoalim.co.il
Organization (O)	Bank Hapoalim Ltd.
Organizational Unit (OU)	Internet department
Serial Number	69:C4:A9:E1:08:67:E1:8F:83:7B:48:4C:97:F8:1D:19
Issued By	
Common Name (CN)	VeriSign Class 3 Extended Validation SSL SGC CA
Organization (O)	VeriSign, Inc.
Organizational Unit (OU)	VeriSign Trust Network
Validity	
Issued On	17/11/10
Expires On	16/02/13
Fingerprints	
SHA1 Fingerprint	E5:B9:5D:91:7A:F3:CE:45:AD:4F:70:9A:55:C2:28:4D:7C:CE:78:AE
MD5 Fingerprint	E1:46:15:99:8E:C6:AE:08:F3:2E:1A:40:0E:A2:58:D1

<u>רשת אמון</u>

השיטה השנייה לבניית תשתית מפתחות ציבוריים מסתמכת על האמון שקיים בין אנשים באופן טבעי. בשיטה זו כל גורם ברשת משמש הן כרשות מאשרת והן כמשתמש. הרשת החברתית שנוצרת בצורה כזאת מבטיחה את אמינותם של המפתחות.

לדוגמה, אברהם רוצה להעביר ליצחק הודעה מוצפנת. אברהם, שמכיר את מתקפת האדם שבאמצע, מעוניין לוודא את אמינותו של המפתח שיצחק שלח לו. במקרה, חבר משותף של השניים, יעקב, נפגש עם יצחק, ומחזיק בעותק של המפתח המקורי. כאשר הוא נפגש עם אברהם, הוא נותן לו את המפתח האמין, וכעת לאברהם יש ערוץ תקשורת בטוח אל יצחק.

שיטה זו נקראת רשת אמון. למעשה, אברהם נתן אמון ביעקב, עקב ידידותם, וסמך עליו כגורם מאשר למפתח של יצחק. שיטת רשת האמון מתבסס על עיקרון זה, אך בקנה מידה גדול בהרבה. כאן, במקום להעביר את המפתח עצמו, המפתחות נמצאים על שרת מפתחות מרכזי, וכל אדם שווידא את זהותו והמפתח של אדם אחר, חותם על המפתח ומעלה את החתימה לשרת. כעת, אם אברהם ירצה לשלוח ליצחק מכתב, הוא יוכל להוריד את המפתח הציבורי שלו, ולראות את כל החתימות שבוצעו עליו. במקרה זה, כאשר יראה שאנשים אמינים (כמו יעקב, שרה, רחל ולאה) חתמו עליו, הוא יוכל לתת בו אמון מסוים.

בתורו, אברהם יחתום על מפתחות של אנשים אותם הוא מכיר, ואנשים שמכירים אותו יחתמו על המפתח שלו. ברשת אמון, אנו נותנים אמון במפתח גם עקב שרשרת של קשרים אישיים: אם אברהם חתם על המפתח של יצחק, ויצחק חתם על המפתח של יעקב, אברהם יוכל לסמוך על המפתח של יעקב.

צורה זו פחות בטוחה, כיוון שאין לנו אפשרות לדעת האם יצחק אכן בדק כראוי את זהותו של יעקב. לעומת זאת, אם יצחק, שרה ורחל חתמו על המפתח של יעקב, ואברהם סומך על כולם, ניתן יהיה לסמוך על המפתח של יצחק.

ובנושא זה רצוי להבחין בין שני סוגי אמון - אמון באדם כמשתמש ברשת, כלומר אמון שהוא אכן מי שהוא טוען שהוא, ושהמפתח אכן שלו, לבין אמון באדם כרשות מאשרת, שבשבילו צריך לבדוק האם האדם ראוי לאמון, ויבדוק היטב כל משתמש ומפתח ברשת לפני שיחתום עליו.

מסיבת חתימת מפתחות

כיוון שבחיי היום-יום רובנו לא מסתובבים עם עותקים של טביעת האצבע של המפתח הפומבי שלנו, ולא מכירים הרבה אנשים שמשתתפים ברשת אמון כזו או אחרת, אין לנו הרבה הזדמנויות לחתום על מפתחות ולשפר ולהרחיב את הרשת.

לשם כך נוצרו מסיבות חתימת מפתחות. מסיבת חתימת מפתחות הנה בעצם מפגש חברתי, בו מתרכזים אנשים (ובעיקר גיקים) לצורך חתימה על מפתחות ציבוריים. כל משתתף מקבל עוד לפני (או בתחילת) המסיבה רשימה של כל המשתתפים, וטביעות האצבע (Key fingerprint) של המפתחות שלהם.

במהלך המסיבה, כל משתתף אמור לזהות את עצמו בפני כל האחרים בעזרת תעודת זהות, רישיון נהיגה או דרכון (ולעתים אף באמצעות תעודת חוגר), ולהקריא את טביעת האצבע של המפתח שלו. שאר המשתתפים מוודאים את זהות האדם, ואת זהות המפתח שלו, ומסמנים זאת בטופס.

לאחר המסיבה, כל משתתף מגיע למחשב בטוח (בעיקר נטול רוגלות), ומוודא לפי הרשימה את טביעות האצבע של המפתחות שברשותו. אם טביעות האצבע תואמות, הוא חותם על המפתח ובכך מאשר את אמינותו. לאחר מכן, ניתן להעלות את המפתחות החתומים לשרת ציבורי.

סיכום

במאמר זה הצגתי את שיטת רשת האמון, ואת רעיון מסיבת חתימת המפתחות. למעשה, שימוש נכון ברשת אמון (ובתנאי שהיא בהיקף גדול מספיק) עשוי להוות צורת תקשורת מהימנה למרבית השימושים.

יתכן שלאחר קריאת המאמר התעורר בכם החשק להקים או להצטרף לרשת אמון. נהדר! בישראל ישנה רשת אמון ותיקה ומוערכת של קהילת הלינוקס והקוד הפתוח, אשר עורכת מסיבת חתימת מפתחות מדי שנה בכנס הקוד הפתוח "אוגוסט פינגווין", וחבריה ישמחו לחתום הדדית על מפתחות כמעט בכל עת, וכמובן שישנן (וניתן להקים) רשתות נוספות לאנשים עמם אתם בקשר.

שימו לב, שככל שיותר אנשים יהיו קשורים לרשת אמון כזו או אחרת, כך תגדל יעילותה של הרשת הגלובלית. רצוי מאוד ליצור קשרים בין רשתות קטנות, ובייחוד מול גורמים בחו"ל. כל קשר כזה מספק תקשורת מהימנה לאנשים רבים.

על המחבר

עמיחי פרץ קלופשטוק, בן 18, עוסק באבטחת מידע מזה כשנה וחצי, חובב לינוקס ותוכנה חופשית, ומתנדב בקבוצת dc9723.