digital whisper
Technologic Papers

שיטות אימות מתקדמות

מאת יובל סיני

מבוא

מהו "אימות"?

פירוש המושג "אימות" באבטחת מידע, כפי שמופיע בוויקיפדיה:

"באבטחת מידע, אימות היא הדרך לזהות את המשתמש ממנו מגיע מסר למערכת ממוחשבת, כך שתימנע אפשרות של התחזות ותסכל התקפת אדם שבתווך. זיהוי זה משמש למטרות שונות:

- קביעת אמינות המידע.
- קביעת זכויותיו של שולח המסר, תוך מניעת זכויות אלה ממי שאינם מורשים להן.
- לצורך משפטי: באמצעות חתימה אלקטרונית ניתן להוכיח בבית המשפט שמכתב מסוים אכן נשלח על ידי המשתמש שחתום עליו, וכך ניתן לחתום על חוזים דרך רשת האינטרנט, ללא פגישה אישית עם החותם.

ניתן לבצע אימות לפי שלושה קריטריונים:

- זהות האדם.
- חפץ בבעלות האדם.
- ידע של האדם.

כאשר נחוץ זיהוי ברמת ודאות גבוהה, נעשה שימוש במספר אמצעי אימות השייכים לקריטריונים שונים. פעולת אימות אלקטרונית שמתבצעת בהיקף רחב החל מהרבע האחרון של המאה העשרים היא זו המשמשת למשיכת כספים ממכשיר בנק אוטומטי. לזיהוי המושך משמש שילוב של שני אמצעים: כרטיס מגנטי שעליו מוטבע זיהוי של המושך, והקשה של סיסמה הידועה רק למושך. גניבה של רק אחד משני אמצעים אלה אינה מאפשרת התחזות.

במקרים שפעולת האימות היא פחות קריטית, נהוג להסתפק באמצעי זיהוי אחד בלבד. בשעון נוכחות די, בדרך כלל, בהעברת הכרטיס המגנטי, ואין צורך ללוות זאת בסיסמה. בכניסה לאתרי אינטרנט רבים, ובכלל זה ויקיפדיה, די בהקלדת זיהוי משתמש וסיסמה, ואין צורך באמצעי זיהוי פיזי. כרטיס מגנטי הוא אמצעי אבטחה נפוץ, אך ניתן לזייפו. כאשר נחוץ זיהוי ברמת ודאות גבוהה, ניתן להחליף את הכרטיס המגנטי בזיהוי ביומטרי, שאותו קשה יותר לזייף. זיהוי ביומטרי הוא זיהוי על-פי תכונות ביולוגיות של המשתמש, כגון טביעת אצבע, סריקת רשתית או בדיקת דנ"א."

מטרת המאמר הינה לספק סקירה כללית של שיטות אימות מתקדמות אשר זמינות כיום לארגונים, תוך הצגת החסמים אשר עכבו את מימוש שיטות האימות המתקדמות בארגונים. כמו כן, המאמר מציג מספר שיטות אימות הנחשבות בעיני רבים כמתקדמות וכמאובטחות, למרות שבפועל אין כך הדבר.

אקדים את המאוחר ואציין כי אין מטרת המאמר לכלול את כל שיטות האימות המתקדמות הקיימות בשוק. כמו כן, אין המאמר מתיימר להציג תיאור טכני מפורט של שיטות האימות אשר מוצגות בו. בנוסף, מן הראוי לציין כי אין במאמר משום המלצה טכנית ו\או משפטית, והמשתמש במידע עושה זאת על אחריותו הבלעדית.

לשם הנוחות, בסוף המאמר מצורפת רשימת ביבליוגרפיה ענפה אשר יכולה לסייע לקורא להעשיר את ידיעותיו בתחום.

חסמים ארגוניים בפני הטמעת טכנולוגיות אימות מתקדמות

ארגונים רבים משתמשים כיום בשיטות אימות קונבנציונליות, אשר מסתמכות בין השאר על שימוש בשם משתמש וסיסמה, ולעיתים בטכנולוגית סיסמה חד פעמית (OTP - One Time Password). לצד החסרונות הרבים אשר קיימים בעת שימוש בשיטות אימות קונבנציונליות, ניתן למנות מספר חסמים עיקריים אשר מנעו עד כה מארגונים רבים להטמיע שיטות אימות מתקדמות:

א. העדר מתודולוגיה של ניהול סיכונים בארגון:

ארגונים רבים אינם מנהלים מתודולוגיה של ניהול סיכונים בארגון, ולפיכך אינם מודעים לאיומים הקיימים בעולם המחשוב. הגישה הניהולית השכיחה אף קובעת כי עדות על "פריצה" למערכות המחשוב בארגון כוללת בחובה נזק הניתן לזיהוי, וזאת בניגוד למציאות העובדתית והמשפטית שבה מקרי "פריצה" רבים אינם מתגלים ב"זמן אמת", אלא רק בדיעבד.

כך לדוגמא, ניתן לראות כי שיטות "ריגול תעשייתי" ו"ריגול בין מדינות" מתבססות לא פעם על עקרון גניבת זהות של עובד הארגון \ המדינה המתחרה, וזאת לשם השגת גישה למידע אשר גילויו יאפשר השגת עליונות על הצד השני. כלומר, מטרתו של הגורם העוין אינה לשתק את מערכות הצד השני, אלא נהפוך הוא - מטרתו של הגורם העוין הינה לאסוף מידע לאורך זמן.
דוגמא אחרת ניתן לראות בתוצאות #OpIsrael Day - 7.4.2013, כאשר קבוצות תקיפה שונות טענו כי הצליחו להשיג גישה לתיבות הדואר הציבוריות של משטרת ישראל, ובכלל זה לתיבת הדואר של לשכת המפכ"ל.

תאימות:

תאימות אפליקטיבית ותשתיתית נדרשת לשם הטמעה מוצלחת של פתרונות אימות מתקדמים. כך לדוגמא, ניתן לראות כי ישנן מערכות הפעלה שאינן תומכות בשימוש באלגוריתמים מתקדמים ובכך אינן מתאימות להטמעת טכנולוגיות אימות מתקדמות. לפיכך, עלות ביצוע ההתאמות הנדרשות מהווה מחסום בלתי עביר עבור ארגונים רבים, דבר אשר מונע את הטמעת טכנולוגיות אימות מתקדמות.

ב. סיבוכיות טכנולוגית:

עד לתקופה האחרונה, הטמעת טכנולוגיות אימות מתקדמות היוותה משימה אשר נחשבה לא פעם כבלתי אפשרית לארגון שאינו ארגון Enterprise (כדוגמת: צבא, מוסדות ציבוריים). לפיכך, ארגונים רבים נמנעו מראש לבחון הטמעת טכנולוגיות אימות מתקדמות, ובכך חשפו את עצמם לסיכונים אשר נובעים משימוש בשיטות אימות קונבנציונליות.

ג. אי התאמה לדרישות העסקיות של הארגון:

כלל ידוע הינו כי יש לאזן בין דרישות אבטחת המידע לדרישות העסקיות (תפעוליות) של הארגון. עם זאת, פתרונות האימות אשר היו זמינים עד לפני מספר שנים מנעו מארגונים יכולת הטמעה של מספר שיטות אימות שונות למשתמש, ובכך יצרו מחסום בפני הטמעת טכנולוגיות אימות מתקדמות. לפיכך, נדרשו עוד מספר שנים על מנת לראות את קיומם של מוצרי מדף אשר מאפשרים לארגון לנהל מספר שיטות אימות שונות למשתמש מממשק ניהול אחיד, וזאת בהתאם לפרופיל הגישה הרצויים (VPN, LAN וכדומה).

ד. תקורת תחזוקה והטמעה:

הטמעת טכנולוגיות אימות מתקדמות חייבה את הארגון בעבר להשתמש בגורמי סיוע חוץ ארגוניים, דבר המייקר את עלות ההטמעה ותחזוקה כפתרון. כמו כן, ארגונים נאלצו לשקלל בעלות הכדאיות של הטמעת פתרון אימות מתקדם עלויות משנה, כדוגמת רכישת רישוי ורכיבי חומרה (כדוגמת: Smart Card), דבר אשר היווה חסם בפני קבלת החלטה לאימוץ טכנולוגית האימות הרצויה.

השפעת המחשוב הנייד וה-Bring your own device (BYOD)

מכשירי ה-Smart Phones, IPad ומקביליהם נהפכו לכלי רב תכליתי בידי אנשים פרטיים וארגונים. לצד אימוץ גישת ה-BYOD, ארגונים נאלצים כיום להתמודד עם מגוון טכנולוגיות, אשר מטרתן לאפשר לעובד ו\או ללקוח הארגון להתחבר למערכות המחשוב של הארגון לשם ביצוע עבודות שגרה. כך לדוגמא, גישה למערכות פיננסיות יכולה להתבצע כיום מציוד מחשוב נייד, ואף גישה ע"י ממשק מוצפן (VPN) לארגון זמינה כיום ממגוון רחב של ציודי מחשוב.

לפיכך, ניתן לראות כי עד לתקופה האחרונה מרבית שיטות האימות אשר שימשו לגישה ממכשירים ניידים לשירותים שכיחים אף הם התבססו על שיטות אימות קונבנציונליות. עם זאת, ניתן לראות כי לאחרונה החלה מגמה של אימוץ טכנולוגיות אימות מתקדמות יותר ע"י ארגונים, וזאת משלושה מניעים עיקריים:

- רצון הארגון לצמצם את תקורת התחזוקה למערכות האימות הקיימות.
- רצון הארגון להגביר את רמת מהימנות ואמינות הליך האימות.
- דרישת לקוחות עסקיים של הארגון לשימוש בזיהוי חד ערכי בגישה למשאבים, תוך התבססות על מימוש שיטות אימות המאפשרות אימות מתקדם מממכשירי מובייל, כדוגמת Smart Phone.
- מעבר לסביבות מורכבות, המחייבות מימוש של שירותי Federation (כדוגמת "סביבות הענן") / SSO (Single sign-on), אשר כוללים בחובם אפשרות למימוש שיטות אימות מתקדמות.

השפעת הרגולציה והמשפטיזציה

את השפעת הרגולציה והמשפטיזציה ניתן לחלק לשני מישורים אשר לכאורה סותרים אחד את השני: מצד אחד, הרגולציה והמשפטיזציה מהווה חסם בפני ארגונים בדרישה לשימוש בשיטות אימות מתקדמות (כדוגמת שימוש באימות ביומטרי), אך מצד שני הרגולציה והמשפטיזציה מטילה חבות על ארגונים לאמת באופן חד ערכי את המשתמש במשאבי הארגון - מבלי לפגוע בפרטיות העובד. כמו כן, לצד הרגולציה והמשפטיזציה יש לזכור כי ארגונים נאלצים להתמודד עם איומים גוברים ונשנים, אשר כוללים ניסיונות כגון גניבת זהו, פרטי של העובד; לקוח המתחבר למשאבי המחשוב.

כמענה לסוגיות שצוינו לעיל, במרבית המקרים ארגונים יכולים להשתמש בתהליכים סטנדרטיים אשר קיימים ברגולציה והמשפטיזציה, כדוגמת ההנחיות המשפטיות הנכללות פס"ד איסקוב, לשם יצירת מענה הולם בין דרישות האבטחה, לדרישות הגנת הפרטיות של העובד. ובמילים אחרות, במרבית המקרים ארגונים יכולים לממש כיום שיטות אימות מתקדמות, אשר יכולות לענות לדרישות האבטחיות-עסקיות.

מבוא ל-Risk-Based Authentication (RBA)

Risk-based authentication (RBA) (אימות מבוסס סיכון) הינה גישה מתודולוגית הטוענת כי יש להתאים את רמת האימות בגישה למשאב המחשוב, וזאת בהתאם למספר פרמטרים:

א. הנזק אשר יכול להיגרם מכשל באבטחת הליך האימות ו\או גישת לא מורשים למשאב המחשוב.

ב. הסבירות שגישה למשאב נתון עלול לגרום לחשיפתו לאיום.

לפיכך, בעת שימוש בגישת "אימות מבוסס סיכון" - העיקרון השולט הינו כי ככל שרמת הסיכון עולה, כך תהליך האימות צריך להיות יותר מקיף ומגביל. להמחשת הגישה המתודולוגית, נשתמש בדוגמא הבאה:

בארגון פלונית ישנה מערכת Webmail הנגישה מהאינטרנט ומנוהלת ע"י ספק צד שלישי, והיא מכילה תכנים שיווקיים-ציבוריים בלבד . מערכת נוספת אשר קיימת בארגון הינה מערכת CRM (Customer Relationship Management) אשר נגישה מהאינטרנט, אשר מכילה פרטי לקוחות ועסקאות.

לאחר ביצוע הליך "ניהול סיכונים" בארגון הנ"ל נקבע כי:

- הנזק אשר יכול להיגרם מכשל באבטחת הליך האימות ו\או גישת לא מורשים למשאב המחשוב - CRM > Webmail.
- הסבירות שגישה למשאב נתון עלול לגרום לחשיפתו לאיום - CRM > Webmail.
- לפיכך, ניתן לשקול מימוש שתי שיטות אימות שונות ומדורגות:
- גישה למערכת ה-Webmail ע"י שם משתמש + סיסמה. במידה שעובד הארגון יהיה מעוניין לגשת למערכת ה-CRM הוא יאלץ לבצע הזדהות נוספת ע"י שימוש באמצעי ביומטרי המותקן על המכשיר הנייד של העובד ("הזדהות חזקה").
- גישה למערכת ה-CRM ע"י שימוש באמצעי ביומטרי המותקן על המכשיר הנייד של העובד ("הזדהות חזקה"). כמו כן, במידה שעובד הארגון עבר אימות ביומטרי מוצלח, הוא יוכל לגשת למערכת ה-Webmail ללא צורך בביצוע אימות נוסף.

המסקנה בעת שימוש בגישת "אימות מבוסס סיכון" הינה כי יש לבצע הלימה בין דרישות האבטחה לבין הדרישות העסקיות-תפעוליות, ובכך לאפשר לארגון גמישות תפעולית לצד שמירה על רמת אבטחה ניאותה. כמו כן, גישת "אימות מבוסס סיכון" מאפשרת קביעת רמת אימות על סמך מספר פרמטרים מצטברים (וזאת ע"פ המשקל היחסי של כל פרמטר אימות), וזאת בניגוד לגישה הקונבנציונלית אשר קבעה את שיטת אימות ע"פ סיווג המערכת בלבד.

להמחשת הגישה המתודולוגית של קביעת רמת אימות על סמך מספר פרמטרים מצטברים, נשתמש בדוגמא הבאה:

בארגון פלונית ישנה מערכת Webmail הנגישה מהאינטרנט ומרשת הארגון דרך שרת Reverse Proxy.

א. כאשר עובד ניגש למערכת ה-Webmail מרשת הארגון הוא מזוהה באופן שקוף ע"י מספר פרמטרים:

- חברות המחשב ב-Active Directory Realm ספציפי.
- קיום Kerberos Authentication Ticket תקף למשתמש שמקורו ב-Active Directory Realm ספציפי.
- כתובת ה-IP של מחשב העובד נכללת בטווח כתובות ה-IP הפנימיות של הארגון.

ב. כאשר עובד ניגש למערכת ה-Webmail מהאינטרנט הוא מזוהה ע"י מספר פרמטרים:

- Client Certificate המזהה את המחשב, כמחשב השייך לארגון. ה-Reverse Proxy מוודא כי התעודה הדיגיטלית אינה במצב Revoke.

- User Certificate המזהה את המשתמש שעובד ארגון. ה-Reverse Proxy מוודא כי התעודה הדיגיטלית אינה במצב Revoke.
- כתובת ה-IP של מחשב העובד אינה נכללת בטווח כתובות ה-IP הפנימיות של הארגון.

לסיכום, ניתן לראות כי שימוש ב-Risk-based authentication (RBA) (אימות מבוסס סיכון) מטשטש את הגבולות המסורתיים בין המושג "אימות" (Authentication) למושג "מתן הרשאות" (Authorization).

שיטות אימות מתקדמות

GPS Location & Geo Location

שיטת אימות זו מתבססת על איסוף שני פרמטרים:

- **Geo Location** - כתובת ה-IP של רכיב המחשוב אשר ממנו נעשה החיבור למשאב המחשוב, והמרתו (בסיוע טבלת המרה) למיקום גיאוגרפי (בד"כ ברמת מדינה ומחוז), הכולל את פרטי ספק האינטרנט (ISP).
- **GPS Location** - מכשירי Smart Phone, IPad ודומיהם מכילים מנגנון GPS פנימי, אשר מכיל יכולות Geo Location מורחבות. כלומר, מעבר לכתובת ה-IP ופרטי ספק האינטרנט (ISP), ניתן להגיע לרמת דיוק הקובעת את מיקום רכיב המחשוב אשר ממנו נעשה החיבור למשאב המחשוב ברמת רזולוציה גבוהה (בעלת מרחב סטייה של מתחת לכ-10-12 מטרים ביחס למיקום האמיתי של רכיב המחשוב אשר ממנו נעשה החיבור למשאב המחשוב).
- ראוי לציין כי לצד היתרונות בשימוש בשיטת אימות זו, יש לשים לב לדרישות החוק ולחובת הארגון לבצע "גילוי נאות" בפני הגורם אשר מתחבר למשאב המחשוב. כמו כן, יש לזכור כי הגורם המתחבר למשאב המחשוב יכול לנטרל בכל זמן נתון את מנגנון ה-GPS הפנימי.

Extensions to Kerberos Protocol

פרוטוקול Kerberos, אשר במקור תוכנן בשנות ה-90 של המאה הקודמת זכה בשנים האחרונות למספר עדכונים ושיפורים:

Kerberos Pre-Authentication [Kerberos Armoring (FAST)]:

הרחבה זו נועדה להתגבר על שתי חולשות שהתגלו בפרוטוקול Kerberos:

א. בסיוע Offline dictionary attack גורם העוין יכול לזהות את תוכן מפתח הקידוד הנכלל ב--AS Request, ובכך הוא יכול לבצע Logon כמשתמש עצמו.

ב. גורם העוין יכול לבצע התחזות ל-KDC ולזייף Kerberos errors, ובכך לחייב את מערכת ההפעלה, אשר תומכת ב-SPNego וממנה המשתמש מבצע את האימות, להשתמש בפרוטוקולי אימות חלשים יותר, כדוגמת NTLM.

כהערת אגב, מן הראוי לציין כי יצרנים מסוימים השתמשו בהרחבה זו לשם הרחבת יכולות נוספות, כדוגמת ניהול ACL (Access List) פרטני לגישה למערכות קבצים. עם זאת, תיתכן בעיית תאימות בעת ביצוע אינטגרציה בין יצרנים שונים, ולפיכך יש לבדוק סוגיה זו לפני החלטה על ביצוע אינטגרציה מסוג זו.

תיקון להרחבה Public Key Cryptography for Initial Authentication in Kerberos (PKINIT):

במקור פרוטוקול Kerberos לא תמך באימות המבוסס על התקני אימות חיצוניים, כדוגמת Smart Card. לשם הוספת תמיכה לשימוש בהתקני אימות חיצוניים, פותחה הרחבה לפרוטוקול ה-Kerberos בשם PKINIT (RFC4556). עם זאת, במהלך השנים התגלה כי ניתן לשלוח דרך ההרחבה בקשת AS_REQ ישנה, וכי ה-KDC לא מוודא כי בקשה זו עדכנית, ובכך ה-KDC מאפשר לגורם עוין להשיג גישה למשאבי המחשוב.

ראוי לציין כי במהלך השנים יצרנים שונים הציגו פתרונות שונים לסוגיה, אך ככל הידוע לא הושגה הסכמה גורפת בין כלל היצרנים, ולפיכך כל יצרן בחר במימוש הרצוי לו, ולפיכך תיתכן בעיית תאימות בעת ביצוע אינטגרציה בין יצרנים שונים הממשים את פרוטוקול ה-Kerberos.

Two-Hop Kerberos Authentication:

בעת מימוש Two-Hop Kerberos Authentication, שרת ביניים יכול לבצע התחזות (Impersonation) למשתמש אשר פנה אליו במקור (ע"י שימוש ב-Kerberos Ticket של משתמש מקור), וזאת לשם גישה למשאב יעד באמצעות פרטי המשתמש המקורי.

כך לדוגמא, משתמש בשם "Test1" ניגש לשרת Web ומציג בפניו את ה-Kerberos Ticket שלו. שרת ה-Web "לוקח" את ה-Kerberos Ticket של המשתמש "Test1", ומציג אותו לשרת ה-Database. כלומר, שרת ה-Database "אינו מודע" לכך שמי שניגש אליו הוא הוא שרת ה-Web, ומספק לשרת ה-Web הרשאות גישה למסדי הנתונים, וזאת בהתאם להרשאות גישה של משתמש "Test1".

חשוב לציין כי Two-Hop Kerberos Authentication מונע זיהוי וודאי של המשתמש שביצע את הפעולה (מבחינת Digital Forensic), וזאת מכיוון שגורם נוסף קיבל "האצלה" (Delegation) להשתמש ב- Kerberos Ticket של המשתמש המקורי.

הערה: רכיבי חומרה רבים (כדוגמת מדפסות) התומכים ב-Two-Hop Kerberos Authentication מחייבים פעמים רבות מימוש של ההרחבה Key Cryptography for Initial Authentication in Kerberos (PKINIT) .

Picture Password:

Picture Password מהווה שיטה אימות חלופית לשיטת הסיסמאות הקונבנציונלית. אשר במקור פותחה לשם מענה לסוגיות הבאות:

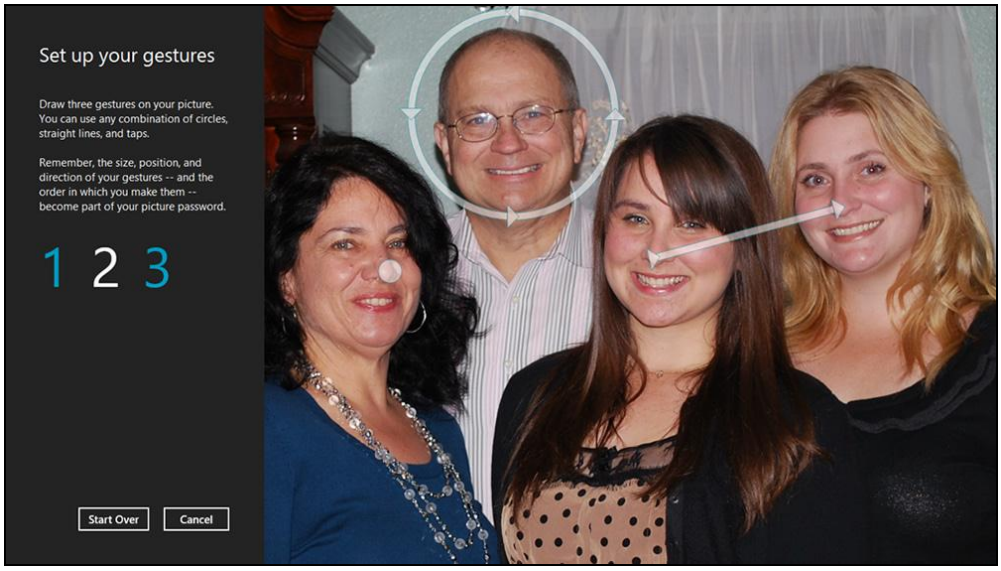
א. מתן אפשרות למשתמש לזכור את הסיסמה, ובכך לצמצם את הסיכון לחשיפת הסיסמה לגורמים חיצוניים.

ב. העלאת רמת האבטחה של הליך האימות. כך לדוגמא, Picture Password המכילה 6 נקודות יחוס בתמונה, שוות ערך לסיסמה רגילה שאורכה 9 תווים.

ג. צמצום קריאות משתמשים למרכז התמיכה (Help Desk), ובכך להקטין את תקורת התמיכה בגין ניהול סיסמת משתמשים.

ד. צמצום יכולתם של כלי Key Loggers לזיהוי סיסמת המשתמש.

מימוש Picture Password בסיסי נכלל באופן מובנה ב-Windows 8, והוא מאפשר למשתמש לבחור תמונה בעלת מספר נקודות יחוס שעליו לזכור, כחלופה לסיסמה המורכבת מתווים ומספרים. נקודות הייחוס מומרות לתוצר אלגוריתם מתמטי, המבטא את סיסמת המשתמש.



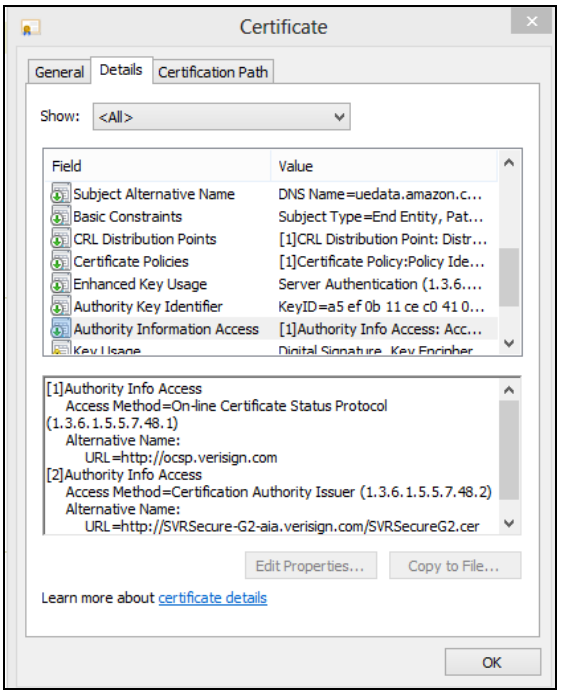
מימוש מתקדם יותר של Picture Password שכיח כיום בשוק ה-IDM (Identity Management), ומאפשר למשתמש לבחור "משפחה" של תמונות (חיות, מכוניות וכדומה), אשר מהן המשתמש צריך לבחור מספר נקודות יחוס. לפיכך, כשלב מקדים להקלדת ה-Picture Password, המשתמש צריך לבחור את ה"משפחה" הנכונה, ורק לאחר מכן הוא יכול לבצע את הליך האימות המלא. לפיכך, ניתן לראות כי ישנה

הרחבה של האלגוריתם המתמטי הנ"ל, ולפיכך המימוש בפועל מחייב שימוש באלגוריתמים מסובכים יותר.

תשתית PKI (Public Key Infrastructure)

Online Certificate Status Protocol (OCSP):

Online Certificate Status Protocol (OCSP) הינו WS (Web Service) המאפשר לוודא ב"זמן אמת" את תקפות תעודה דיגיטלית ש"ישות" (Principal) מציגה בעת הליך אימות ו\או הצפנה. כך לדוגמא, בעת ניסיון אימות של משתמש לאתר אינטרנט ע"י תעודה דיגיטלית, אתר האינטרנט יכול לוודא ב"זמן אמת" כי התעודה הדיגיטלית של המשתמש אינה במצב Revoke. להלן מצ"ב צילום מסך של התעודה הדיגיטלית של אחד משירותי חברת Amazon המוגן ב SSL ומכיל הפניה לשרת המאפשר ביצוע בדיקת תקינות תעודה דיגיטלית ע"י שימוש ב-Online Certificate Status Protocol (OCSP):



היתרונות העיקריים בעת שימוש ב-Online Certificate Status Protocol (OCSP) ביחס לשיטה הקונבנציונלית אשר כוללת בדיקה של תקפות התעודה הדיגיטלית בקובץ CRL (Certificate Revocation List):

- בעת ביצוע Revoke לתעודה דיגיטלית, "העדכון" זמין מידית ללקוחות המעוניינים לבדוק את תקפות התעודה, וזאת בניגוד לשימוש ב-CRL, אשר מתעדכן מספר פעמים ביום. לפיכך, ניתן לראות כי בעת שימוש ב-CRL יתכן כי יעבור זמן רב יחסית עד כי שיתברר כי תעודה דיגיטלית זו אינה תקפה יותר.

- בעת שימוש ב-CRL, מערכות הפעלה שומרות (בד"כ) את תוצאות בדיקת תקינות התעודה ב-Cache בעל TTL (Time to live) ארוך יחסית. לפיכך, שוב ניתן לראות כי בעת שימוש ב-CRL יתכן כי יעבור זמן רב יחסית עד כי שיתברר כי תעודה דיגיטלית זו אינה תקפה יותר.
- השימוש ב-WS (Web Service) מאפשר קבלת זמני תגובה טובים ביחס לשימוש ב-CRL.
- הסיבה לכך נובעת מהעובדה כי על מנת לבדוק את תקפות תעודה דיגיטלית ע"י שימוש ב-CRL, על הצד הבודק להוריד את קובץ ה-CRL ורק לאחר מכן לבצע את פעולת הבדיקה. מכיוון שנפחי קבצי CRL יכול להגיע לגודל של מאות מגה (ולעיתים לגדלים גדולים אף יותר), זמן הורדת הקובץ משפיע ישירות על זמן הבדיקה הכולל.

FIPS 201 PIV-I + II & TPM Virtual Smart Cards

בשנת 2006 שוחרר תקן FIPS 201 PIV-I + II אשר הגדיר ארכיטקטורה ורשימת תהליכים חיוניים לשם ביצוע אימות מאובטח בעזרת התקנים חיצוניים, כדוגמת Smart Card, Biometric Reader, וכדומה.
כאבולוציה לתקן זה פותחה טכנולוגיית Virtual Smart Cards המנצלת את יכולות ה- (Trusted Platform Module) BIOS TPM המאפשרת שמירה מאובטחת של תעודה דיגיטלית (ולעיתים אף תוכנה להנפקת סיסמאות OTP) ב-BIOS במחשב.

לפיכך, ארגונים יכולים לממש היום שיטות אימות מתקדמות, כדוגמת Smart Card ללא צורך ברכישת התקן Smart Card פיסי.

עם זאת, ארגון המעוניין להטמיע ב-Virtual Smart Cards צריך לענות למספר דרישות קדם, כדוגמת:

א. מערכת הפעלה בתחנת העבודה צריכה לתמוך בטכנולוגיית Virtual Smart Cards.
ב. ה BIOS TPM (Trusted Platform Module) בתחנת העבודה צריך לתמוך בתקן (Trusted Computing Group) TCG בגרסה 1.2 ומעלה.

כמו כן, על הארגון המעוניין להטמיע ב-Virtual Smart Cards להכיר היטב את ההבדלים (התפעוליים והאבטחתיים) בין מימוש Virtual Smart Cards למימוש Smart Card פיסי.

שיטות ביומטריות

חלק ניכר משיטות האימות הביומטריות קיימות מזה תקופה בשוק המחשוב, אך לאחרונה ניתן לזהות מספר שיפורים חשובים בתחום זה:

א. הקטנת עלויות מימוש אימות ביומטרי.
ב. כניסת יצרנים נוספים לשוק.

ג. שיפור ביצועים ואינטגרציה עם מערכות (Identity Management) IDM & Directory Services נוספות.

ד. שיפור יחס, False-Positive (הסבירות לאימות משתמש לא מורשה) Positive-False (הסבירות לאי אימות של משתמש מורשה) - ומתן אפשרות לארגון לשלוט על הערכים הרצויים לפרמטרים אלו (Threshold).

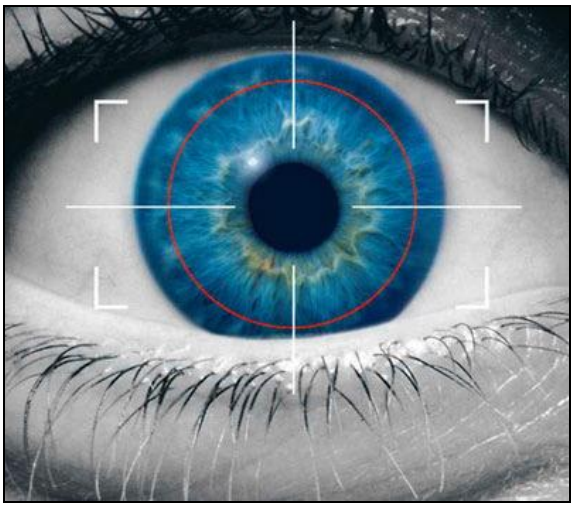
ה. שימוש בטכנולוגיית מחשוב נייד (כדוגמת Smart Phone) לטובת זיהוי ביומטרי, ללא צורך בהוספת רכיבי חומרה נוספים. כפי שצוין קודם לעיל במאמר, ארגונים רבים השכילו להבין את השפעת המחשוב הנייד וה Bring your own device (BYOD).

ו. אימוץ תקינה מוסכמת ע"י יצרני הפתרונות. עם זאת, ראוי לציין כי עדיין נדרשת עבודה רבה בתחום זה.

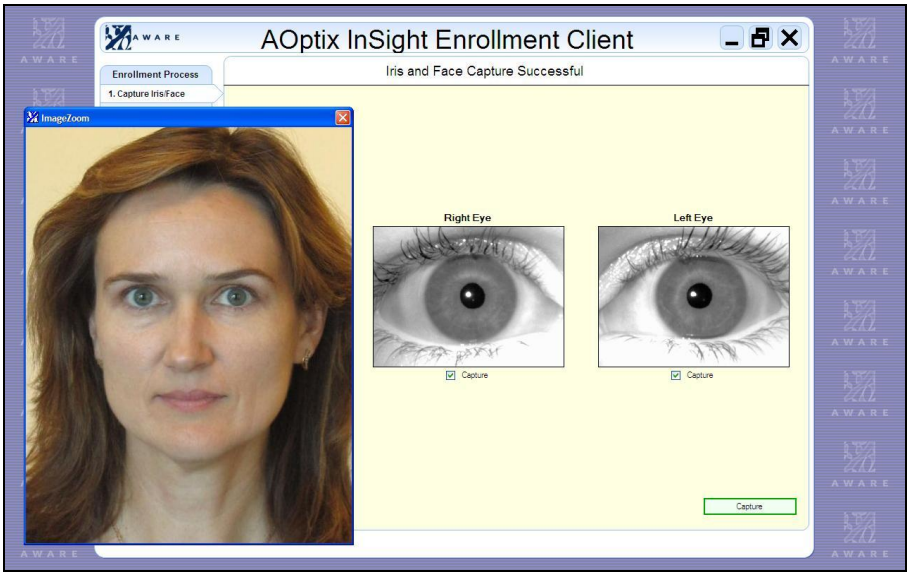
Iris (קשתית העין)

אפיון הליך אימות מבוסס Iris (קשתית העין) נכלל כיום בתקן ISO/IEC 19794-6, וניתן לזהות מספר שיטות מימוש שכיחות בתחום זה. עקרון שיטת אימות זו מתבסס על זיהוי המבנה הלוגי-פיסי השוכן מאחורי קרנית העין - הקשתית. הקשתית היא טבעת של שרירים, ובמרכזה נמצא חור האישון (הדומה לצמצם המצלמה). תפקיד הקשתית הוא לשלוט בכמות האור שנכנס לעין. היא עושה זאת על ידי התכווצות והתרפות - כשהקשתית מתכווצת האישון קטן, ולעין מגיעה כמות קטנה יותר של אור. הקשתית מקנה לעין את צבעה.

בעת ביצוע אימות, מאפייני הקשתית מומרים ע"י אלגוריתם לפרמטרים מתמטיים (בד"כ בסיוע הקרנה של קרן אינפרה אדומה חלשה), ומשווים לערך השמור במערכת האימות.



מצ"ב דוגמא למערכת אימות ביומטרי Iris (קשתית העין) מבית חברת AOptix המאפשרת ביצוע אימות Iris ממכשירי Smart Phones:



דוגמא נוספת הינה מימוש אימות ביומטרי Iris (קשתית העין) מבית חברת AOptix בשערי מסוף גבולות:

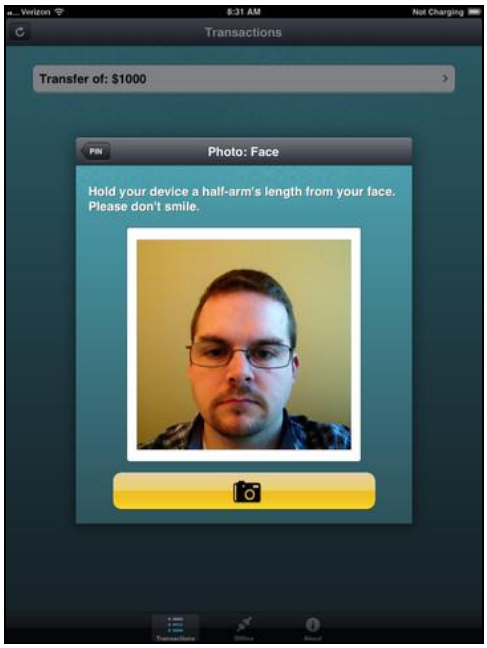
הערה: אימות מבוסס Iris (קשתית העין) שונה מאימות מבוסס Retina, וזאת מכיוון שאימות מבוסס Retina מבוסס על זיהוי מאפיינים ומבנים של כלי הדם בעין, דבר המאפשר לאמת ברמת וודאות גבוהה יותר את הישות המזדהה. עם זאת, מימוש אימות מבוסס Retina נחשב למסובך יותר טכנית, וכשלים באימות שכיחים כתוצאה מבעיות רפואיות של האדם המזדהה. כמו כן, עלות מערכות אימות מבוססות Retina גבוהה משמעותית מעלות מערכות אימות המבוססות על אימות Iris (רשתית העין).

Face & Face live-ness detection (blinking, lip movement, head movement):

אפיון הליך אימות מבוסס Iris (רשתית עין) נכלל כיום בתקן ISO/IEC 19794-4, וניתן לזהות מספר שיטות מימוש שכיחות בתחום זה.

בעת ביצוע אימות Face מתבצע הליך קורלציה בין תמונתו של אדם השמורה במערכת האימות לבין תמונה המשודרת אל מערכת האימות, וזאת בסיוע אלגוריתם מתאים. מכיוון שישנה אפשרות לזייף בקלות יחסית את תמונתו של הישות המזדהה, פותחה טכנולוגיה בשם Face live-ness detection & blinking, lip movement, head movement המאפשרת לבדוק "חיות" של אדם (כדוגמת זיהוי מאפייני תנועת ראש), ובכך להגדיל את הסבירות כי הישות המזדהה הינו אדם.

מצ"ב דוגמא למערכת אימות ביומטרי מבית חברת Daon המאפשרת ביצוע אימות Face live-ness detection (blinking, lip movement, head movement) ממכשיר Smart Phone:



Voice biometric matching & Voice live-ness detection (ASR, randomized phrases):

בעת ביצוע אימות Voice מתבצע הליך קורלציה בין חתימת קול אדם השמורה במערכת האימות לבין תמונה המשודרת אל מערכת האימות, וזאת בסיוע אלגוריתם מתאים. מכיוון שישנה אפשרות לזייף בקלות יחסית את קולו של הישות המזדהה, פותחה טכנולוגיה בשם Voice live-ness detection (ASR , randomized phrases) המאפשרת לבדוק "חיות" של אדם (כדוגמת זיהוי תבניות שפה, מבטא, "סלנג"), ובכך להגדיל את הסבירות כי הישות המזדהה הינו אדם.

מצ"ב דוגמא למערכת אימות ביומטרי מבית חברת Daon המאפשרת ביצוע אימות Voice live-ness randomized phrases ,ASR detection ממכשיר טלפון נייד:

- ASR - Automatic Speech Recognition.

:Voice Biometrics Technology to Expand Fraud Prevention & Emergencies

מערכות מבוססות Voice Biometrics Technology to Expand Fraud Prevention & Emergencies מאפשרות לבצע אימות מתקדם, וזאת בסיוע טכנולוגיית NLP - (Natural Language Processing).

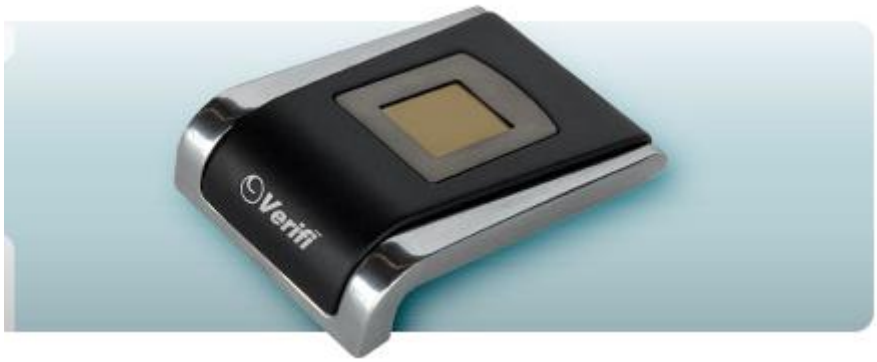
טכנולוגיית NLP - (Natural Language Processing) מאפשרת לזהות את המצב הנפשי של האדם הפונה לארגון, כדוגמת מצבי לחץ ומצוקה, כעס. כמו כן, טכנולוגיית NLP - (Natural Language Processing) מסייעת לזהות מצבים שבו ישנו ניסיון לביצוע הונאה, כדוגמת ניסיון התחזות. ראוי לציין כי מערכות מבוססות טכנולוגיית NLP - (Natural Language Processing) קיימות מזה תקופה במספר מוקדי שירות בארץ, וכי הטכנולוגיה שפותחה ע"י חברת NICE הישראלית נחשבת לחלוצה בתחום זה.

:Fingerprint & Live Finger Detection

בעת ביצוע אימות Fingerprint (טביעת אצבע) מתבצע הליך קורלציה בין חתימת טביעת אבצע של אדם השמורה במערכת האימות לבין הטביעת האצבע המשודרת אל מערכת האימות, וזאת בסיוע אלגוריתם

מתאים. טכנולוגיית Live Finger Detection מהווה הרחבת יכולות ביצוע אימות מבוסס Fingerprint (טביעת אצבע), וזאת מכיוון שטכנולוגיה זו מעלה את הסבירות כי הישות המזדהה הינה אדם.

מצ"ב דוגמא למערכת אימות ביומטרי מבית חברת Zvetco Biometrics המאפשרת ביצוע אימות Live Finger Detection:



[P6000 Fingerprint Device ,Zvetco Biometrics]

- קיימים בשוק כיום פתרונות לביצוע אימות מבוסס Fingerprint (טביעת אצבע) ממכשירי Smart Phones - ללא צורך בהוספת רכיבי חומרה נוספים.

Finger Vein:

בעת ביצוע אימות Finger Vein (זיהוי תבניות של כלי דם באצבע האדם) מתבצע הליך קורלציה בין חתימת תבנית של כלי הדם באצבע של אדם, לצילום השמור במערכת האימות, וזאת בסיוע אלגוריתם מתאים. היתרון הבולט בין מימוש אימות Finger Vein (זיהוי תבניות של כלי דם באצבע האדם) למימוש אימות Fingerprint & Live Finger Detection הינו סוג המידע הנשמר במערכת האימות, הנחשב "לפחות רגיש". כמו כן, מחקרים שבוצעו בארה"ב גילו כי שיטת אימות זו נתפסת כפחות פולשנית, ולפיכך רמת ההתנגדות של לקוחות ועובדים לשימוש בשיטה זו נמוכה משמעותית ביחס לרמת ההתנגדות של לקוחות ועובדים אשר נדרשים להשתמש בשיטות אימות ביומטריות חלופיות.

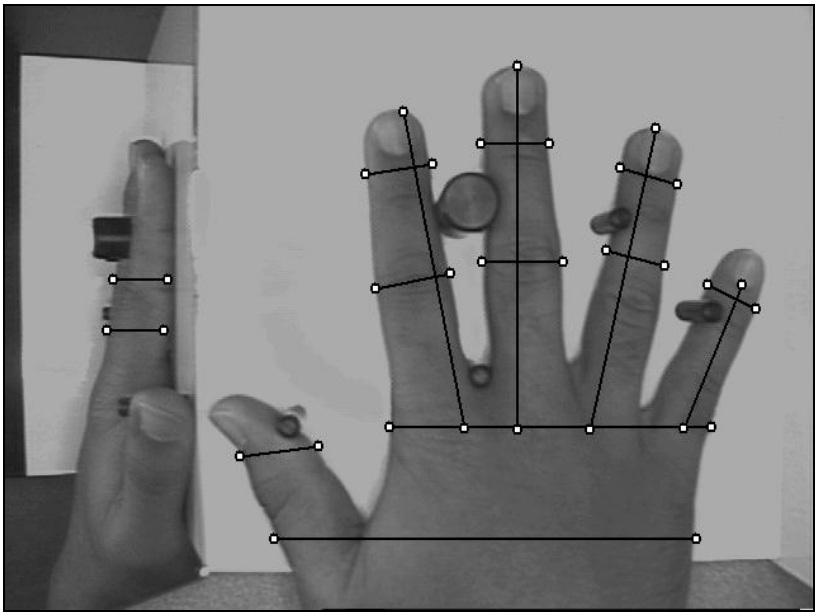
אם נשווה את רגישות הנתונים השמורים במערכות האימות הביומטריות השכיחות בשוק, נוכל לראות כי גם אם תתרחש חשיפה לא מבוקרת של מידע השמור במערכת הניהול של פתרון אימות מבוסס Finger Vein (זיהוי תבניות של כלי דם באצבע האדם), הפגיעה הצפויה בפרטיות האדם שפרטיו נחשפו צפויה להיות מינימלית, מה שגם הסיכוי להשתמש במידע שנחשף להפללת אדם חף מפשע שואף לאפס. לפיכך, ניתן לראות כבר כיום מימוש של שיטת אימות Finger Vein (זיהוי תבניות של כלי דם באצבע האדם) במספר גופי בריאות בארה"ב - המשרתים מספר רב של מטופלים.

מצ"ב דוגמא למערכת אימות Finger Vein (זיהוי תבניות של כלי דם באצבע האדם) מבית חברת M2SYS:

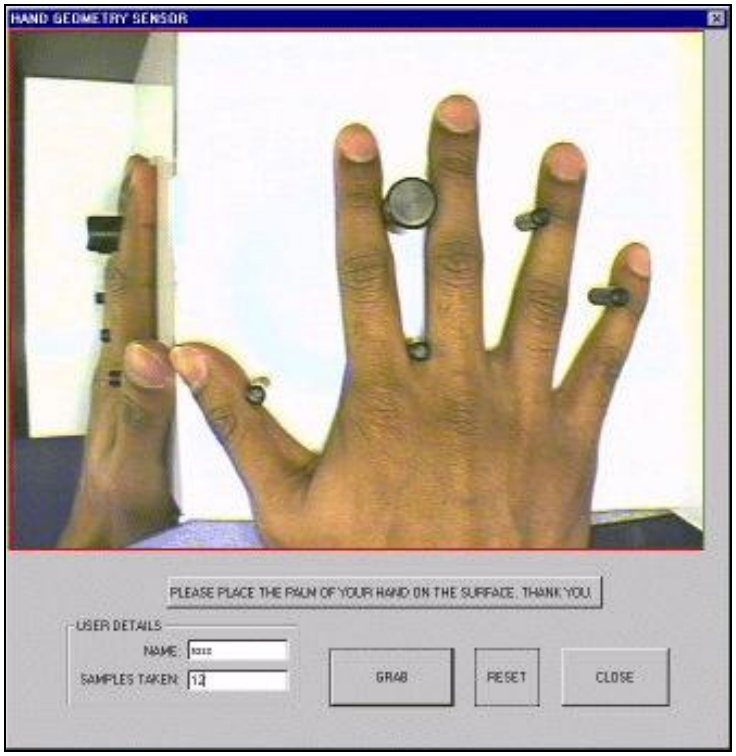
Hand-based Personal Authentication / Hand Geometry:

בעת ביצוע אימות Hand-based Personal Authentication / Hand Geometry (אימות מבנה כף היד) מתבצע הליך קורלציה בין חתימת מבנה כף היד (ע"פ מספר פרמטרים כדוגמת: אורך האצבעות, עובי האצבעות, רוחב האצבעות, המרחק בין האצבעות) של אדם השמורה במערכת האימות לבין מבנה כף היד של אדם המשודרת אל מערכת האימות, ממשטח מערכת האימות המכיל את חיישני האימות, וזאת בסיוע אלגוריתם מתאים.

מצ"ב דוגמא למשטח מערכת אימות המכיל את חיישני האימות:



מצ"ב דוגמא לממשק ניהול מערכת אימות Hand-based Personal Authentication / Hand Geometry (אימות מבנה כף היד):



[הערה: ניתן לראות מימוש של שיטת אימות זו בבנקטים בהודו לדוגמא.]

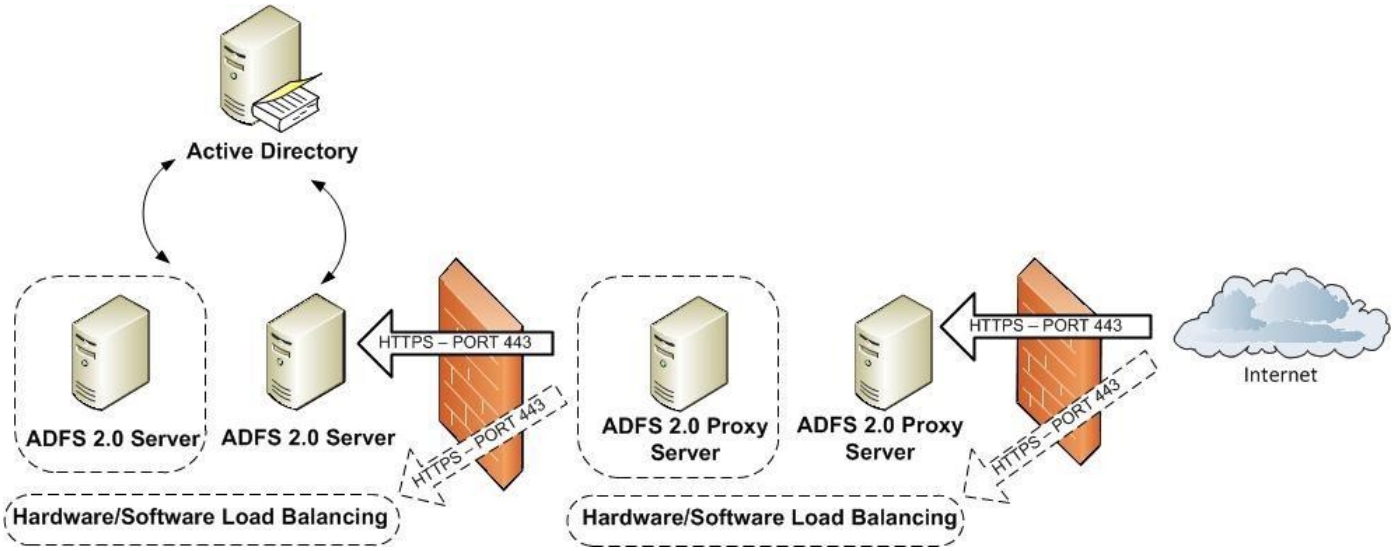
2.1 SAML (Security Assertion Markup Language):

SAML הינו XML-based framework (הגרסה העדכנית ליום כתיבת מאמר זה הינה 2.1) המאפשר ניהול אחיד בין ממשקים משותפים של מערכות מחשוב, דבר הכולל ניהול של המתודות הבאות:

- אימות משתמש.
- מתן תכונות משתמש.
- התממשות למערכת ניהול הרשאות למשתמש (בד"כ מערכת ניהול הרשאות התומכת בתקנים 3.0 XACML ו\או OAUTH 2.0).

כך לדוגמא, שימוש ב-SAML Token מאפשר מימוש SSO (Single Sign On) בין Active Directory Forest המותקן ברשת הארגון, לבית שירות "ענן" Office 365. לשם הגדלת מהימנות ואמינות ה-SAML Token , ניתן לבצע חתימה דיגיטלית של SAML Token. כמו כן, ביצוע חתימה דיגיטלית של ה-SAML Token מאפשר ביצוע Mutual authentication or two-way authentication בין השותפים הממשים ביניהם SSO (Single Sign On).

עם זאת, מן הראוי לציין כי SAML הנו תקן פתוח, שאינו תלוי יצרן כזה או אחר.



איך לא לבצע אימות מתקדם

חלק זה במאמר סוקר מספר טעויות שכיחות בעת ביצוע אימות.

UDDI \ IMEI:

בדומה ל-MAC address (Media Access Control Address), למכשירים ניידים ישנה כתובת זיהוי ייחודית (לכאורה) הממומשת ע"י שתי שיטות מימוש שכיחות: UDDI ו-IMEI (International Mobile Station Equipment Identity). עם זאת, התגלה בתקופה האחרונה כי ניתן לזייף את כתובות הזיהוי הנ"ל בקלות, ולפיכך ההמלצה כיום היא להימנע מלהסתמך על שיטות המימוש הנ"ל.

תעודות זהות חכמות:

החל מינואר 2013 ממשלת ישראל מבצעת "פיילוט" של פרויקט תעודות זהות חכמות, וזאת חרף הסיכונים הגבוהים במימוש התצורה הנוכחית של המאגר הביומטרי. לפיכך, מן הראוי להזכיר את דבריו של פרופ' אלי ביהם, דיקן הפקולטה למדעי המחשב בטכניון:

> "העובדה ששיטת העמעום שהציע פרופ' עדי שמיר, שמטרתה להפחית את דליפת הפרטיות מהמאגר הביומטרי, לא נבחרה לשימוש על ידי משרד הפנים בטענה המגוחכת שהיא פוגעת בפרטיות, מוכיחה שכוונת מקימי המאגר אינה מניעת זיופי זהות, כדברי החוק, אלא קידום מטרות זרות שאינן מוזכרות בחוק".

סיכום

המאמר סקר בתחילתו את עקרונות האימות, וכן את הקשיים אשר עמדו בפני ארגונים אשר שקלו לאמץ שיטות אימות מתקדמות. כמו כן, המאמר סקר מספר שיטות אימות מתקדמות, וכן סקר מספר שיטות אימות הנחשבות לטענת רבים מתקדמות ומאובטחות, אף בפועל חושפות את הארגון ו\או משתמש הקצה לאיומים לא סבירים. בנוסף, המאמר הציג את מתודולוגיית Risk-based authentication (RBA) (אימות מבוסס סיכון) אשר הינה המתודולוגיה המומלצת כיום לשימוש בעת תהליך קבלת החלטות על מימוש שיטת אימות כזו או אחרת.

על המחבר

יובל סיני הינו מומחה אבטחת מידע, סייבר, מובייל ואינטרנט, חבר קבוצת SWGDE של משרד המשפטים האמריקאי.

ביבליוגרפיה

ביבליוגרפיה כללית:

- ISO Standards Catalogue:

http://www.iso.org/iso/home/store/catalogue_ics.htm

- Guide to Integrating Forensic Techniques into Incident Response Recommendations:

http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

- פס"ד טלי איסקוב ואח' נ' אפיקי מים אגודה חקלאית שיתופית לאספקת מים בבקעת בית שאן בע"מ ואח', עע 90/08, עע 312/08:

http://www.moital.gov.il/NR/rdonlyres/689B0383-5FA7-4AC8-B964-11D974DD1AD2/0/isakov.pdf

ביבליוגרפיה בנושא Kerberos:

- How the Kerberos Version 5 Authentication Protocol Works:

http://technet.microsoft.com/en-us/library/cc772815.aspx

- RFC 4556 - Public Key Cryptography for Initial Authentication in Kerberos (PKINIT):

http://www.ietf.org/rfc/rfc4556.txt

- RFC 6113 - Generalized Framework for Kerberos Pre-Authentication [Kerberos Armoring (FAST)]:

http://tools.ietf.org/html/rfc6113

- Security implications in Kerberos by the introduction of smart cards:

http://www.cosic.esat.kuleuven.be/publications/article-2188.pdf

- Understanding Kerberos Double Hop:

http://blogs.technet.com/b/askds/archive/2008/06/13/understanding-kerberos-double-hop.aspx

ביבליוגרפיה בנושא Picture Password:

- Picture Password: A Visual Login Technique for Mobile Devices, NISTIR 7030, 2003:

http://csrc.nist.gov/publications/nistir/nistir-7030.pdf

- Signing in with a picture password:

http://blogs.msdn.com/b/b8/archive/2011/12/16/signing-in-with-a-picture-password.aspx

ביבליוגרפיה בנושא PKI (Public Key Infrastructure):

- RFC 2560- Online Certificate Status Protocol (OCSP):

http://www.ietf.org/rfc/rfc2560.txt

- FIPS PUB 201-1, PERSONAL IDENTITY VERIFICATION (PIV) OF FEDERAL EMPLOYEES AND CONTRACTORS, 2006:

http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

- Understanding and Evaluating Virtual Smart Cards:

http://www.microsoft.com/en-us/download/details.aspx?id=29076

ביבליוגרפיה בנושא אימות ביומטרי:

- Chin-Chuan Han, A hand-based personal authentication using a coarse-to-fine strategy, 2004:

http://www.sciencedirect.com/science/article/pii/S0262885604001155#

- Face Image Analysis by Unsupervised Learning (The Springer International Series in Engineering and Computer Science), Marian Stewart Bartlett, Springer; Softcover reprint of the original 1st ed. 2001 edition (October 26, 2012).
- Raed Sahawneh1, Ahmed Ibrahim2, Sami Qawasmeh3, Arwa Zabian3, Authentication Method Using Hand Images for Access Control systems, International Arab Journal of e-Technology, Vol. 1, No. 4, June 2010.
- Dont Blink:Iris Recognition for Biometric Identification:

http://www.sans.org/reading_room/whitepapers/authentication/dont-blink-iris-recognition-biometric-identification_1341

- Applications expand for biometrics:

http://www.securityinfowatch.com/blog/10852181/applications-expand-for-biometrics

- Zvetco Biometrics ,P6000 Fingerprint Device Zvetco Biometrics:

http://www.zvetcobiometrics.com/Products/P6000/overview.php

- Palm Scanners Debut at Lehigh Valley Hospital:

http://salisbury.patch.com/articles/palm-scanners-debut-at-lehigh-valley-hospital

- RightPatient™ Biometric Patient Safety System:

http://www.m2sys.com/healthcare/rightpatient-biometric-patient-safety-system/

- Finger Vein Biometrics Identification for Membership Management Software:

http://blog.m2sys.com/membership-management/finger-vein-biometrics-identification-for-membership-management-software/

- אמצעי זיהוי ביומטריים במסמכי זיהוי ומאגרי מידע ממשלתיים - סקירה משווה - מוגשת לוועדת החוקה, חוק ומשפט, 14 בינואר 2009:

http://www.knesset.gov.il/mmm/data/pdf/m02179.pdf

- עו"ד יהונתן קלינגר, על זיהוי וסיכונים:

http://2jk.org/praxis/?tag=%D7%AA%D7%A2%D7%95%D7%93%D7%95%D7%AA-%D7%96%D7%94%D7%95%D7%AA-%D7%91%D7%99%D7%95%D7%9E%D7%98%D7%A8%D7%99%D7%95%D7%AA

- אל תיתנו את האצבע למאגר,פרופ' אלי ביהם, 22/04/2012:

http://acheret.co.il/?cmd=articles.528&act=read&id=2722

ביבליוגרפיה בנושא Voice Biometrics Technology to Expand Fraud Prevention & Emergencies:

- NICE Utilizes Voice Biometrics Technology to Expand Fraud Prevention Suite to Contact Centers:

http://maya.tase.co.il/bursa/report.asp?report_cd=789208

ביבליוגרפיה לנושא SAML (Security Assertion Markup Language):

- SAML Wiki Knowledgebase:

http://saml.xml.org/wiki/saml-wiki-knowledgebase

- Tim Harrington, Directory Federation Services (ADFS) 2.0 with Office 365:

http://blogs.catapultsystems.com/tharrington/archive/2011/04/01/active-directory-federation-services-adfs-2-0-with-office-365-part-1-%E2%80%93-planning.aspx