digital whisper
Technologic Papers

מבוא ל-Web 3.0 Security

מאת יובל סיני

מבוא

האינטרנט (מרשתת בעברית) נולד לקראת סוף שנות ה-90 של המאה הקודמת, והיווה עבור רבים רעיון חדשני אך מוגבל בחזונו הראשוני. רבים לא חזו את ההשלכות האדירות של רעיון זה על החברה האנושית ככלל, ועל הסביבה הטכנולוגית כפרט. הצפי המקורי היה שמרבית המשתמשים באינטרנט יהיו אנשי אקדמיה החולקים מידע סטטי ובלתי מסווג ביניהם. כפועל יוצא של הנחות היסוד אלו יוצרי תשתית האינטרנט (והתשתיות הנלוות) לא שמו דגש על סוגיות בתחום אבטחת מידע, לא שכן על סוגיות נוספות כדוגמת ביצועים, ועוד. ניתן למנות מספר גלים טכנולוגיים ועסקיים בתחום האינטרנט (Web):

א. ארכיטקטורת Web 1.0 (The shopping carts & static web):

Web 1.0 מתמקד בהצגת מידע סטטי למשתמש, תוך שמירה על מודל מופשט: M4H (machines for humans) . במילים אחרות, המשתמש ניגש לשרת ה-Web ודולה ממנו תוכן המאוחסן בדפי HTML סטטיים (Rendering in the server side).

ב. ארכיטקטורת Web 2.0 (The writing and participating web):

Web 2.0 מתמקד בהצגת מידע סטטי ודינמי למשתמש תוך תאימות למספר רב של ממשקי לקוח (כדוגמת מובייל), ותוך הרחבת המודל המופשט של Web 1.0 והכללת מתודולוגית: H4M (humans for machines) -> M4H (machines for humans) . כלומר, נוספה היכולת של המשתמש לגשת לשרת ה-Web, לדלות מידע פרסונלי לגביו, וכן נוספה יכולת לדפדפן לבנות ולעצב את דף ה-HTML בצד הלקוח וזאת ע"י שימוש ביכולות מתקדמות, כדוגמת Ajax/JavaScript/CSS/AMD. בנוסף, נוספה יכולת של "לקוח הקצה" לערוך ולפרסם תכנים לאינטרנט באופן עצמאי וכן להשתתף ב"רשתות חברתיות" אשר יצרו "חוויה אנושית-חברתית" חדשה.

ג. ארכיטקטורת Web 3.0 (The semantic executing web):

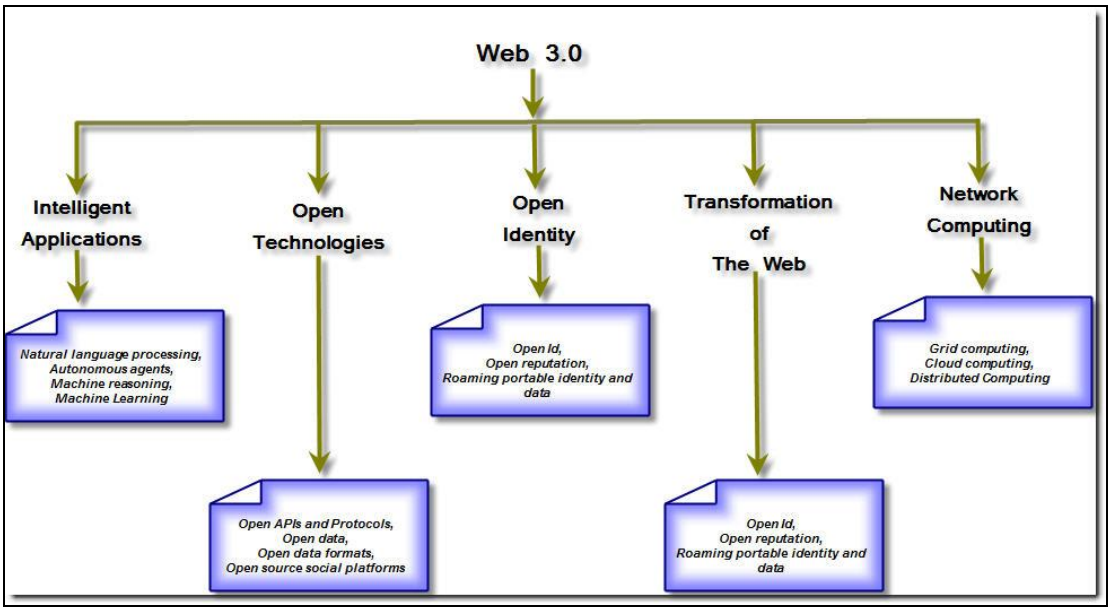
Web 3.0 החל את פעולתו לפני מספר שנים מועטות, ואת אותותיו הראשוניים ניתן כבר לראות במימושים הנכללים בתשתיות מחשוב של חברות ענק כדוגמת Google (e.g. iGoogle) ו- Microsoft (e.g. Bing). גל זה מרחיב את המודל המופשט של Web 2.0 וכולל את מתודולוגית:

H4M (humans for machines) -> M2M (machine to machine) -> M4H (machines for humans)

ארכיטקטורת Web 3.0[1] (The semantic executing web)

ארכיטקטורת ה-Web 3.0 כוללת בחובה את מתודולוגיית H4M (humans for machines) -> M2M (machine to machine) -> M4H (machines for humans) אשר מהווה הרחבה של המודל המופשט של Web 2.0.

לצד הכללת מתודולוגיה זו תחת ארכיטקטורת ה-Web 3.0, ניתן למנות עוד מספר טכנולוגיות על-תשתיתיות אשר ישנו צפי להרחבת השימוש בהם בעתיד הקרוב, וכי הם אלו אשר יהפכו את חזון ה- Web 3.0 למעשה:



בעיון ברשימת הטכנולוגיות על-תשתיתיות ניתן להסיק מספר מסקנות מעניינות:

1. השימוש בשירותי "ענן" יגדל באופן משמעותי, וישנה סבירות גבוהות כי חלק ניכר מהחברות המסחריות ומהגופים הציבוריות יעבירו את תשתית המחשוב שלהם ל"ענן". רוצה לומר, אתרי ה-Data Center המסורתיים ייעלמו ממרבית הארגונים, ואף המושג אגף\מחלקת ה-IT הארגונית תשנה את אופייה.

2. השימוש בתשתית ניהול זהויות הכוללת תמיכה בסטנדרטים פתוחים (כדוגמת Open ID 2.0/3.0 / SAML 2.X) מאפשר השגת גמישות אבטחתית-תפעולית בעת גישה למשאבים ב"ענן" ובמעבר "שקוף" בין התקנים (כדוגמת ניוד Session קיים ממכשיר מובייל למכשיר טאבלט וכל זאת ללא פגיעה ב"חווית הלקוח"). כמו כן, השימוש בתשתית ניהול זהויות התומכת בסטנדרטים פתוחים מאפשר ביצוע אינטגרציה מאובטחת בין תשתית הניהול זהויות של הארגון לבין זו של ספקי השירותים

[1] מכיוון שה Web 3.0 נמצא כיום בשלבי התהוות, יתכן שוני בין המתואר במאמר זה למצב בפועל.

ב"ענן". וכהערת אגב ראוי לציין כי מתודולוגיית H4M -> M2M -> M4H מאפשרת ניתוק של הקשר הישיר בין זהות הלקוח לספק השירות בפועל.

בנוסף, ניתן לראות כי לכל "לקוח הקצה" יוגדר ערך "מוניטין ציבורי" [2](מבוסס פרמטרים כדוגמת: מהימנותו, היסטוריית רכישות, רמת הזדהות, וכדומה היוצרים Risk Scoring לישות). ה"מוניטין ציבורי" "ילך" עם הלקוח בעת גישתו לספקי שירות ותוכן, והוא יאפשר לספקי שירות ותוכן להציע שירותים ופרטי תוכן ייחודיים ל"לקוח קצה". ראוי לציין כי ספקי שירות ותוכן יוכלו להשתמש ב"מוניטין ציבורי" לטובת תהליך "קבלת החלטות" \ "הערכת סיכונים" שבעקבותיו תתבצע חסימת גישה של לקוח לשירותים ותכנים מסוימים. כלומר, יתכן מצב שבו "לקוח הקצה" יהיה מחובר לאינטרנט, אך ספקי התוכן והשירותים יבודדו אותו על בסיס "מוניטין ציבורי" נמוך.

3. השימוש בטכנולוגיות המבוססות על Open Source יגבר, ואף ישנו צפי כי מערכות ההפעלה של משתמשי הקצה יעברו לעבודה ב"תצורה רזה" תוך שימוש במערכת הפעלה אוניברסלית ואחידה בכל ההתקנים. אחד היתרונות הבולטים בעת עבודה עם Open Source הינו יכולת יצירת אינטגרציה שקופה בין פלטפורמות שונות, וכל זאת ללא צורך ברכישת מוצרים ייחודיים ו\או רכש רישוי.
כמו כן, קיים צפי כי השימוש בכסף וירטואלי ו-eWallet יגבר אף הוא, ולפיכך הגופים הפיננסים המסורתיים יחויבו להסתגל לשינויים במציאות החדשה. ניתן לראות כי השימוש ב"כסף וירטואלי" יאפשר ל"לקוח הקצה" שמירה של כספו ב"כספת פרטית" שתאוחסן ב"ענן" ו\או ב"התקן מחשוב" כזה או אחר.

4. השימוש באינטליגנציה מלאכותית יגדל באופן משמעותי, דבר אשר יאפשר שיפור משמעותי באיכות המידע המוצג ל"לקוח הקצה" ע"י מנועי חיפוש ("פרסונליזציה של המידע"). כמו כן, כחלק ממתודולוגיית H4M -> M2M -> M4H ניתן לראות כי "מכונה" מסוגלת כבר כיום להפעיל שיקול דעת (בהתאם לאלגוריתם) ולקבל החלטות הכוללות בין השאר יכולת להפעלת "מכונות" נוספות לשם השגת מידע נוסף ו\או ביצוע פעולה נדרשת.

כהערת אגב, ראוי לציין כי ישנה הפרייה הדדית בין התפתחות ה-"Big Data" להתפתחות יכולות "האינטליגנציה המלאכותית". כך לדוגמא, השימוש ב-MapReduce מאפשר ביצוע חיפוש מהיר על תשתית מבוזרת של Hadoop Cluster הכוללת כמות גדולה של קבצים (כולל קבצים בפורמטים שונים).

[2] הגדרה שכיחה נוספת הינה "רמת אמון". כלומר, אם מערכת X סומכת על ישות בשם Yuval, אזי מערכת Y תסמוך גם על ישות בשם Yuval. עם זאת, אין מדובר במודל אמון המקובל ב-PKI, אלא מדובר על מודל אמון דינמי, דבר המעדכן את "רמת האמון" של לקוח הקצה ב"זמן אמת" וממספר רב של מקורות.

בנוסף, בעיון בספרות המחקרית ניתן ללמוד כי אימוץ טכנולוגיות התשתית הבאות חיוני לשם הצלחת חזון ה-Web 3.0:

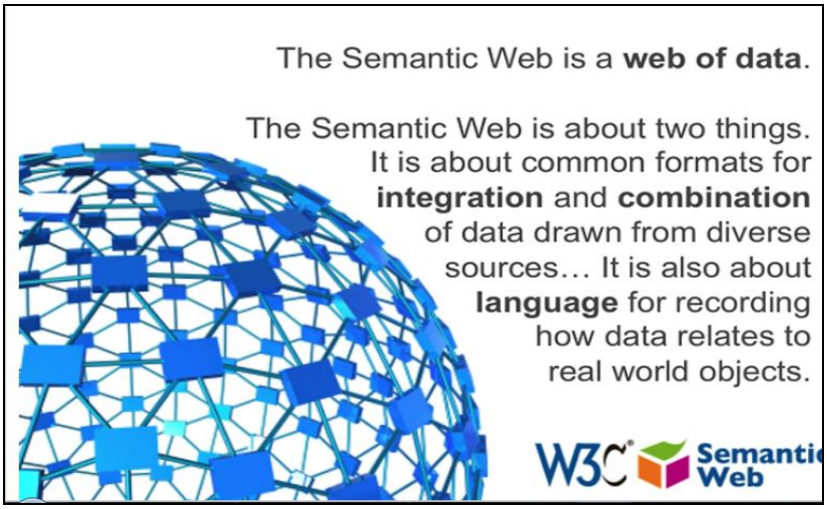
1. פרוטוקול HTTP 2.0, אשר כולל מימוש פרוטוקול בינארי להעברת תעבורת Web, ואשר יש ביכולתו לצמצם את ה-Latency בטעינת מידע, תוך שימוש באלגוריתמי דחיסה וניהול מתקדמים. כמו כן, בניגוד למצב הקיים כיום, שימוש ב-TLS\SSL ב-HTTP 2.0 לא יחייב צריכת פס רוחב גבוהה יותר. ראוי אף לציין כי בניגוד לדעה הרווחת אין צפי כי HTTP 2.0 יחליף את HTTP 1.1, ובאופן ריאלי ישנו צפי ששני הפרוטוקולים ישמשו את תשתית ה-Web (עם זאת, סביר להניח שארכיטקטורת Web 4.0 תשנה את התמונה).

2. השימוש ב-XML tagging and bagging יגבר.

3. ארכיטקטורת Representational State Transfer (REST) תאפשר קיצור זמן פיתוח, ביצוע אינטגרציה יעילה בין פתרונות וכן הגדרת Style לייצוג Objects ובניית Queries.

4. פרוטוקול IP6[3], אשר חיוני לשם מתן מענה לבעיית חוסר כתובות ה-IP הקיים כיום. לאור העובדה שחזון ה-Web 3.0 כולל תקשורת מרובת משתמשים ומרובת התקנים, ניתן יהיה לראות בעתיד הקרוב כי במרבית רכיבי חומרה ייכלל מודול להתחברות לסביבת האינטרנט (כדוגמת כרטיס DLNA תומך IP6).

5. הוספת תמיכה ב-Framework הכולל Symantic Web (metadata)[4] אשר יוטמעו בדפי האינטרנט, ומטרתם לסייע באיתור מידע וביצוע תהליכי פרסונליזציה של מידע (וזאת לפני טעינת הדף ע"י "לקוח הקצה"):



[3] IP6 כולל יכולות IPSEC מובנות בפרוטוקול עצמו, דבר המהווה שינוי משמעותי ביחס למימוש הקיים ב-IP4. למעשה, כל מידע הנשלח ע"י פרוטוקול IP6 אמור להישלח כבחירת מחדל מקודד כ-IPSEC (וזאת בתנאי שהיצרן לא שינה את שיטת העבודה)

[4] כינוי רווח בתחום הארכיונאות לתהליכים מסוג אלו הינו "הדיגיטציה של המידע".

ישנם כבר כיום מספר תקנים המתחרים להגדרת פורמט הSemantic Web- (metadata), כגון:

- RDF - Resource Description Framework
- OWL - Web Ontology Language

Web 3.0 Security

כעת אסקור מספר איומים בתחום אבטחת מידע ופרטיות אשר נובעים מארכיטקטורת ה-Web 3.0. עם זאת, ראוי לציין מספר השגות בנושא:

א. סביר להניח שמרבית (אם לא כל) סוגיות אבטחת המידע אשר נכללות בארכיטקטורת Web 2.0 ימשיכו ללוות אותנו גם בארכיטקטורת Web 3.0. עם זאת, חלק זה לא כולל התייחסות לסוגיות אבטחה אלו, ומטרתו להתמקד בסוגיות אבטחת מידע הנובעות מארכיטקטורת Web 3.0.

ב. יתכנו מימושים שונים לארכיטקטורת ה-Web 3.0, ולפיכך יתכנו איומים נוספים \או איומים שונים, וזאת מעבר לאיומים המוצגים במאמר זה.

ג. התערבות רגולטורים ממדינות השונות ו/או ארגונים בינלאומיים שונים (כדוגמת האיחוד האירופי, האו"ם וכדומה) עשויים להשפיע על מימוש ארכיטקטורת ה-Web 3.0.

ד. מרבית יצרני פתרונות אבטחת המידע ומוצרי המדף אינם מודעים כלל לאיומים הנובעים מארכיטקטורת Web 3.0 והטכנולוגיות החדישות. למען הפרדוקס, ניתן לראות כי הצהרות יצרני פתרונות אבטחת מידע כי הם תומכים בארכיטקטורת Web 2.0 באופן מלא, פעמים רבות אינן מחזיקות מים.

הגנת פרטיות

אחת הדילמות שכל אדם אשר ירצה להשתמש בתשתית המבוססת על ארכיטקטורת Web 3.0 יחווה הינה ה-Trade-off בין ה"שימושיות" לסוגיית הפרטיות. לשם הרחבה בנושא אני ממליץ לקורא לפנות למאמרו של עו"ד יהונתן קלינגר -'הענן והמידע שלך' אשר מרחיב את היריעה בנושא.

מצ"ב רשימה של מספר פרמטרים שכיחים המאפשרים למנוע החיפוש לזהות את המשתמש באופן חד ערכי:

- General Parameters: Geo Location, GPS, ISP Name, IP, Time, Typing rate, Keyboard language/s, DNS-Name, IMEI Number, ESN Number, SIM Card Number, Mobile Phone Number, etc.
- Browser Parameters: Browser Installation Agent, Browser/s Type/s & version/s, Browser add-ons, Camera model & type, microphone model & type, User-Agent (including operating system type & model), Homepage, Logon account (e.g. Gmail account), Cookies, HTTP Referer, Encoding support, Accept-Language, etc.
- Data Parameters: Interests, old queries, common words, data type, data links, common use Language, etc.

המונופול על הידע והבניית המציאות של הפרט

אחד המשפטים הידועים מכתביו של George Orwell ("1984") הינו:

"He who controls the past controls the future. He who controls the present controls the past."

ממשפט זה ניתן להסיק דואליות מעניינת - כשם שניתן לקבוע כיצד יראה העתיד של הפרט והציבור, ניתן באותה מידה לקבוע כיצד יראה העבר של הפרט והציבור. ובמילים אחרות, הנרטיב של העבר והעתיד הינו סובייקטיבי וניתן לבנייה בידי הפרט ו/או גורם אחר. לשם המחשת נכונות משפט זה אני מציע להשתמש בניסוי פשוט:

שאלו "שאלה" במנוע חיפוש אחד, ולאחר מכן שאלו את אותה שאלה במנוע חיפוש שני. בנוסף, השתמשו באותו מנוע חיפוש לביצוע התשאול הנ"ל ממחשב שממוקם במדינת ישראל, ולאחר מכן בצעו את אותו תשאול באותו מנוע חיפוש ממדינה אחרת. במרבית המקרים "התשובות" (תוצאות החיפוש) ל"שאלה" יניבו ערכי חיפוש שונים, למרות שמדובר באותה "שאלה" בדיוק. ובמילים אחרות, ישנו גורם צד שלישי (ולעיתים אף מספר רב של גורמי צד שלישי) אשר בוחר לנו מהו "המידע הנכון" עבורנו. לשם הפרדוקס, חלק ניכר ממשתמשי האינטרנט אינם מודעים (ואף לא פעם הם אינם מעוניינים לדעת) מהן ההשלכות השליליות של ביצוע סינון המידע ע"י הגורמים הנ"ל.

כפי שצוין קודם לעיל, ארכיטקטורת Web 3.0 מרחיבה את יכולת "הדיבור" בין מערכות באינטרנט, ולפיכך רמת הפרסונליזציה של המידע רק תגדל. כלומר, תשתית ה-Web 3.0 תוכל בחלק ניכר מהמקרים לזהות את הישות אשר עומדת מולה באופן חד ערכי, ובכך להציג את "המידע הנכון" עבורו בכל מקום ובכל זמן. ומפה נשאלת השאלה האם "המידע הנכון" הוא אכן נכון עבור הגורם השואל?!
ואסכם את נקודה זו בשתי דוגמאות;

נניח שאתם מחפשים אחר אתר האינטרנט של ארגון פיננסי וגורם עוין מצליח לשנות את תוצאות החיפוש כך שאתם תופנו לאתר Phishing אשר יאפשר לגורם עוין לגנוב את פרטי האימות לגישה לאתר הארגון הפיננסי הנ"ל. אומנם עד כה נראה לכאורה כי לא מדובר באיום חדש, אך השוני בין איום ה-Phishing המסורתי לאיום ה-Phishing החדש הינו שאותו גורם עוין יוכל להסתפק בשינוי נתון השמור במערכת מחשוב אשר מכילה חלק ממידע הפרסונליזציה שלכם, ובכך להציג לכם את אתר ה-Phishing בכל מקום ובכל זמן.
דוגמא אחרת הינה מצב שבו אתם ואחרים מעוניינים לקבל מידע על שער מניה על מנת לבחון כדאיות להשקעה. גורם עוין יוכל לכוון את תוצאות החיפוש כך שכמות גדולה של אנשים יקבלו מידע מוטעה, דבר אשר יאפשר לאותו גורם עוין לבצע "הרצת מניות".

קצרה היריעה מלתאר תרחישים שבהם גורמי כוח וממשל ינצלו את יכולות תשתית ה-Web 3.0 בכדי להשפיע על תוצאת בחירות אלקטרוניות, ועוד. כמו כן, ראוי לציין כי ארכיטקטורת Web 3.0 מאפשרת (ברמה כזו או אחרת) החלת Audit מרכזי ומלא אחר פעילות המשתמשים, דבר אשר מצד אחד יוכל להגביר את רמת האבטחה ברשת האינטרנט, אך מצד שני הדבר פותח פתח לניצול לרעה של מידע זה ע"י גורמים שונים.

Semantic Web Common Web Attack Vulnerability

כפי שצוין בראשית המאמר ה-Semantic Web (Metadata) יוצמדו לדפי האינטרנט על מנת לשפר את איכות החיפוש ודליית המידע (Data Mining). עם זאת, ניתן לנצל את ה- Semantic Web (Metadata) לשם גרימת נזק לגורמים המתשאלים את דפים אלו. לדוגמא: כשל תוכנתי בביצוע תשאול (Parsing) מדפדפן הלקוח יכול לאפשר XSS אשר מקורו מה-Semantic Web (Metadata) המוצמדים לדף. לאור העובדה כי סביר להניח שיהיו מספר תקני Semantic Web (Metadata), וכי מרבית תקני ה- Semantic Web (Metadata) לא שמו דגש על אבטחת מידע הסבירות לבעיות אבטחה מסוג אלו רק תגדל.
דוגמא אחרת הינה מצב שבה מנוע חיפוש יתשאל דף המכיל Semantic Web (Metadata) המכיל מידע עוין, דבר העלול לפגוע בפעילות מנוע החיפוש עצמו.
מן הראוי אף לציין כי קישור מערכות המשתמשות בתקנים שונים לטובת מימוש Semantic Web (Metadata) יכול להוות נקודת כשל אשר תוכל לאפשר לתוקף לבצע מניפולציות וגניבת מידע ביתר קלות.

Eavesdroppers (האזנה לתעבורה)

מתקפה זו אינה חדשה, אך לאור העובדה שהוכח כי ישנן אלגוריתמי הצפנה חלשים המשתמשים בתשתית ה-SSL\TLS של ארגונים רבים, וכן ישנם מימושים להצפנה אשר תוכננו By Design להכיל חולשות מובנות, ניתן להסיק כי מדובר בנקודת כשל אידיאלית לניצול. שילוב נקודת כשל זו לעובדה כי תשתית ה-Web 3.0 תכלול (במרבית המקרים) שימוש בזהות דיגיטלית אחידה[5] של הפרט אשר תשמש אותו להזדהות בפני שרתי תוכן ושירותים תגביר את המוטיבציה של "הגורם העוין" לגניבת הזהות. סביר אף להניח כי "המוניטין הציבורי" של "לקוח הקצה" ישמש שפרמטר יעיל לסינון התעבורה, ובכך ה"גורם העוין" יוכל לאתר בקלות יחסית תעבורה העונה לפרופיל רצוי.

גדילה בשימוש ב-Advanced Persistent Threat (APT)

מזה שנים מספר ניתן לראות גדילה בשכיחות ה-Advanced Persistent Threat (APT) המשמשים לטובת Fraud וגניבת מידע רגיש. סביר להניח כי כניסת תשתית ה-Web 3.0 והטכנולוגיות הנלוות תדרבן את "יצרני" ה-APT בפיתוח יכולות חדשות, תוך ניצול היכולות החדשות. כך לדוגמא ניתן יהיה לראות את קיומם של Coin-Mining Malware מתקדמים אשר יוכלו לסייע לתוקף להפוך מחשבים רגילים ל-" Zombie Computer" אשר ישמשו להפקת מטבעות וירטואליים, כדוגמת Bitcoin. דוגמא אחרת הינה גניבת Bitcoin מ-Wallet המאוחסנים במכשירי ניידים. בנוסף, עולה הסבירות כי יעשה שימוש בגורמי צד שלישי תמים לשם הלבנת כספים אשר נגנבו באופן דיגיטלי.

לפיכך, קיומם של APT ייעודיים, כדוגמת Zeus, SpyEye (אשר מהווים את הדור הראשון של APT) ייהפך לדבר שבשגרה. סביר אף להניח שה-APT החדשים יכללו בנוסף ליכולת לביצוע פעילות פיננסית עוינת, יכולת לגניבת הזהות של "לקוח הקצה". סביר אף להניח כי "המוניטין הציבורי" של "לקוח הקצה" ישמש כגורם אשר יאפשר ל"גורם עוין" לכוון את ה-APT כלפי יעדים ספציפיים ביתר קלות.

שבירת מודל "ניהול הסיכונים" המסורתי

"ניהול הסיכונים" מהווה עבור ארגונים רבים כלי עזר לביזור סיכונים וקבלת החלטות אסטרטגיות המשליכות על נושאים רבים, וביניהם אבטחת מידע והגנת פרטיות. עם זאת, מרבית המודלים של "ניהול הסיכונים" מתבססים על מודל מופשט, שאינו כולל במרבית המקרים התייחסות לפעילות רוחבית הנכללת כחלק מארכיטקטורת ה-Web 3.0 והטכנולוגיות הנלוות. כך לדוגמא, ארגונים רבים יסמכו את ידיהם ב"צורה עיוורת" על ספקי תכנים ושירותים. העדר רגולציה וגורמי אכיפה במרחב הבינלאומי ישאירו את

[5] סוגיית גניבת הזהות אינה חדשה, אך השוני בין המצב כיום למצב ב-Web 3.0 הינו שגניבת זהות תאפשר ל"גורם עוין" להשיג גישה למרבית (אם לא לכל) מידע"לקוח הקצה" \ הארגון המותקף. קל וחומר כי גורם עוין יוכל להשתמש בזהות הגנובה לשם ביצוע פעולות פיננסיות וכדומה לטובתו. ראוי אף לציין כי בעית גניבת הזהות מחריפה לאור העובדה כי מרבית המידע עובר לאחסון בתשתית Big Data הנגישה מכל מקום ובכל זמן.

ארגונים אלו חשופים לאיומים שישנו קושי לכמתם ולהעריכם (ובכך ליצר "הערכת סיכונים"). לפיכך, סביר להניח שארגונים אלו ניסו להשית את הסיכונים הנובעים ממציאות עסקית-טכנולוגית זו על "לקוחות הקצה".

לפיכך, נדרשת הרחבה של מודל "ניהול הסיכונים" המסורתי על מנת לכלול שקלול רב-ממדי של סיכונים הנובעים מהאיומים החדשים הנכללים בארכיטקטורת ה-Web 3.0 והטכנולוגיות הנלוות. בנוסף, מודל "ניהול הסיכונים" החדש יצטרך לספק מענה לארכיטקטורות וטכנולוגיות חדשות.

ארכיטקטורת Web 4.0 (Open, Linked & Symbiotic Web)

ארכיטקטורת Web 4.0 צפויה לתפוס תאוצה החל משנת 2020, וסביר להניח כי היא תכלול בחובה אתגרים חדשים בתחום אבטחת מידע והגנת הפרטיות. ניתן לראות מימושים ראשונים של ארכיטקטורת Web 4.0 כבר כיום, כדוגמת פרויקט DBpedia[6]:

> "DBpedia is a crowd-sourced community effort to extract structured information from Wikipedia and make this information available on the Web. DBpedia allows you to ask sophisticated queries against Wikipedia, and to link the different data sets on the Web to Wikipedia data. We hope that this work will make it easier for the huge amount of information in Wikipedia to be used in some new interesting ways. Furthermore, it might inspire new mechanisms for navigating, linking, and improving the encyclopedia itself."

הצפי הינו כי ארכיטקטורת Web 4.0 תוכל לשפר ולהוסיף מספר ממשקים עיקריים:

א. קישור בין מידע אישי / מקור מידע שאינו פומבי למידע ציבורי לשם ביצוע תשאול מתקדם, וזאת תוך מתן אפשרות להפיכת המידע האישי / מקור המידע שאינו פומבי למידע הנגיש לכלל הציבור ו\או לקבוצת משתמשים ספציפית.

ב. הוספת יכולת להוספת מידע אישי לאובייקט המציג מידע ציבורי ביתר קלות, ובכך לשפר את איכות תוצאות החיפוש לכלל הציבור ו\או לקבוצת משתמשים ספציפית. כחלק מתפיסה זו הצפי הינו כי יינתן לכל אובייקט (כולל ל-Metadata) כתובת URL ייעודית.

ג. הצמדת "Personal Agent" תוכנתי לכל אדם, ובכך להציג מידע הרלוונטי אליו באופן אישי. קרי, אין מדובר בתפיסה של מערכת חיפוש מרכזית אשר אוגרת מידע על הישות מהצד, אלא מדובר ברכיב תוכנה אינטגרלי אשר יוצמד לכם אדם.

[6] מקור הציטטה: http://dbpedia.org/About

ד. קישור מתקדם בין אדם למכונה - כדוגמת גרסה מתקדמת של המשקפיים של חברת Google, אשר יש ביכולת ממשק זה ליצור עולם וירטואלי-פיסי חדש.

סיכום

המאמר כלל סקירה כללית של הארכיטקטורות Web 1.0 - 4.0, תוך התמקדות בארכיטקטורת Web 3.0. כמו כן, המאמר הציג מספר סוגיות בתחום אבטחת מידע והגנת הפרטית אשר נובעות מקיומה של ארכיטקטורת ה-Web 3.0 והטכנולוגיות הנלוות. לצד היתרונות הגלומים בארכיטקטורות והטכנולוגיות החדשות ניתן למנות מספר רב של חסרונות אשר יש לתת לגביהן את הדעת.

"The future is not set"

Terminator 2: Judgment Day, 1991

על המחבר

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

ביבליוגרפיה

ביבליוגרפיה כללית:

- Architectural Styles and the Design of Network-based Software Architectures, Dr. Roy Thomas Fielding:
  http://www.ics.uci.edu/~fielding/pubs/dissertation/top.html
- Eli Pariser: Beware online "filter bubbles":
  http://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles.html
- Project Page: Vulnerability Analysis of the Wombat Voting System by Bar Perach and Guy Lando:
  http://course.cs.tau.ac.il/secws12/projects/wombat-analysis
- HOW TO CALCULATE INFORMATION VALUE FOR EFFECTIVE, SECURITY RISK ASSESSMENT, Mario Sajko, Kornelije Rabuzin, Miroslav Bača Faculty of organization and informatics, Varaždin, Croatia Web 1.0 vs Web 2.0 vs Web 3.0 vs Web 4.0 - A bird's eye on the evolution and definition:
  http://flatworldbusiness.wordpress.com/flat-education/previously/web-1-0-vs-web-2-0-vs-web-3-0-a-bird-eye-on-the-definition/
- Dbpedia Project:
  http://dbpedia.org/About
- The Evolution of the Web - From Web 1.0 to Web 4.0 Dr. Mike Evans School of Systems Engineering University of Reading:
  http://www.cscan.org/presentations/08-11-06-MikeEvans-Web.pdf
- Judge dismisses suit against Google for bypassing Safari privacy settings:
  http://www.theverge.com/2013/10/10/4825350/judge-dismisses-suit-against-google-for-bypassing-safari-privacy

גן השבילים המתפצלים, חורחה לואיס בורחס, הוצאת הקיבוץ המאוחד, 1975.

ביבליוגרפיה בנושא HTTP 2.0:

- Hypertext Transfer Protocol version 2.0, draft-ietf-httpbis-http2-06:
  http://tools.ietf.org/html/draft-ietf-httpbis-http2-06
- SPDY and What to Consider for HTTP/2.0, Mike Belshe:
  http://www.ietf.org/proceedings/83/slides/slides-83-httpbis-3

ביבליוגרפיה בנושא Web 3.0:

- Web 3.0: The Third Generation Web is Coming:
  http://lifeboat.com/ex/web.3.0
- Security and Privacy on the Semantic Web:
  http://www.olmedilla.info/pub/2007/2007_book-sptmdm.pdf
- EMERGING PAYMENTS FRAUD TRENDS, Limor S Kessem, RSA FraudAction Technical LeadWhy Should You Care About Web 3.0? Dr San Murugesan Director, BRITE Professional Services Adjunct Professor, University of Western Associate Editor in Chief, IEEE IT Professional, Sydney, Australia.

ביבליוגרפיה בנושא אבטחת מידע ב-Web 3.0:

- The Evolution of Targeted Attacks in a Web 3.0 World, Posted by Tom Kellermann in Cloud, Cloud-based Security, Securing the Cloud:
  http://cloud.trendmicro.com/the-evolution-of-targeted-attacks-in-a-web-3-0-world/
- Software [In]security: Securing Web 3.0, Gary McGraw:
  http://www.informit.com/articles/article.aspx?p=1217101

ביבליוגרפיה בנושא Big Data:

- What is MapReduce?
  http://www-01.ibm.com/software/data/infosphere/hadoop/mapreduce/
- Building big data? Are you building a security headache too?
  http://www.theregister.co.uk/2013/08/19/big_data_security_considerations/

ביבליוגרפיה בנושא אבטחת מידע והגנת פרטיות ב"ענן":

- 'הענן והמידע שלך' מאת עו"ד יהונתן קלינגר:

http://www.digitalwhisper.co.il/files/Zines/0x13/DW19-3-Coulds.pdf

- אבטחת מידע בעולם העננים' מאת: עידו קנר ואפיק קסטיאל:

http://www.digitalwhisper.co.il/files/Zines/0x1B/DW27-5-CloudsSecurity.pdf

- תקני אבטחת מידע במחשוב ענן, מאת שחר גייגר מאור:

http://www.digitalwhisper.co.il/files/Zines/0x29/DW41-2-Cloud_Regulation.pdf

פיצול מידע בשירותי ענן, מאת מריוס אהרונוביץ':

http://www.digitalwhisper.co.il/files/Zines/0x2B/DW43-3-Cloud.pdf