digital whisper Technologic Papers

מבוא להתקפת ערוץ צדדי (Side-Channel Attack)

מאת יובל סיני

מבוא

מערכות המחשוב פועלות באינטראקציה הדדית מול הסביבה החיצונית. לדוגמא, מערכת המחשוב עשויה לפלוט אוויר חם לסביבה (משתנה פיזיקאלי א'), ובמקביל מערכת המחשוב עשויה לקלוט אוויר קר מהסביבה (משתנה פיזיקאלי ב'). דוגמא אחרת הינה פליטת רעש (משתנה פיזיקאלי) לסביבה החיצונית מרכיבים מכניים ו/או שמע המובנים במערכת המחשוב; מאוורר, דיסק-קשיח מכני, רמקולים, אוזניות, וכו'.

בהתאם למחקרים אקדמיים שונים, נלמד כי מדידה של אותם משתנים 'חיצוניים' / 'צדדיים' הנפלטים לסביבה (כדוגמת משתנים פיזיקאליים), ולאחר מכן ביצוע פעולות הסקה ישירות ו/או עקיפות (כדוגמת ניתוח סטטיסטי) על סמך אותם משתנים, ניתן לאבחן את מצב (State) של מערכת המחשוב ברגע נתון.

לשם הפשטה של עקרון זה, ניתן להשתמש בדוגמא מעולם הספורט. על מנת לדעת אם שער הובקע (מצב), ניתן לבחון את מהלך המשחק במישרין (באופן ישיר), וזאת ע"י ראיה בפועל של המשחק. עם זאת, ניתן לדעת זאת אף בצורה עקיפה (לא ישירה / 'חיצונית' / 'צדדית'), וזאת על ידי בחינת רף השינוי בשמע האקוסטי הבוקע מהאצטדיון, כאשר ניתן להקיש כי בסמיכות לזמן הבקעת שער בפועל, הרעש אשר האוהדים יפיקו יגדל באופן משמעותי במימד הזמן והעוצמה.

על בסיס עקרון זה מבוססת התקפת ערוץ צדדי (באנגלית: Side-Channel Attack); ניצול העובדה כי ניתן למדוד משתנים 'חיצוניים' / 'צדדים' בפעילות מערכת מחשוב (מדידת הפלט של מערכת מחשוב לסביבה), להחיל מודל חישובי מתאים על אותם משתנים, ובכך לקבל מידע ערכי לגבי המצב (State) של מערכת המחשוב.

ויקפידיה, האנציקלופדיה החופשית מספקת את ההגדרה הבאה להתקפת ערוץ צדדי[1]: "התקפה קריפטוגרפית המנצלת מידע שמושג מאופן היישום הפיזי או השימוש של מערכת ההצפנה ולא בדרך של כוח גס המופעל כנגד האלגוריתם עליה היא מבוססת או קריפטואנליזה תאורטית. לעתים, בשל מגבלות

[1] מקור: https://he.wikipedia.org/wiki/%D7%94%D7%AA%D7%A7%D7%A4%D7%AA_%D7%A2%D7%A8%D7%95%D7%A5_%D7%A6%D7%93%D7%93%D7%99, נדלה ב-14.12.2016

טכניות ואף בשל רשלנות או חוסר תשומת לב באופן יישום מערכת ההצפנה, נוצרות נקודות תורפה המאפשרות חילוץ מידע העלול לסכן את ביטחון המערכת כולה."

עם זאת, בעיון בספרות המחקרית ניתן ללמוד כי ניתן לנצל את התקפה זו לשם מיצוי מידע ערכי מעולמות תוכן נוספים, וזאת כדוגמת מיצוי מידע ערכי מעולם הווירטואליזציה (Virtualization), וזאת על סמך תשאול מצב (State) של מכונה וירטואלית (Virtual Machine) פלונית, ממכונה וירטואלית (Virtual Machine) אלמונית, כאשר שתי המכונות הווירטואליות (Virtual Machines)) מתארחות על אותו Hypervisor.

יצוין כי באמצעות שימוש בהתקפה זו תוקפים עשויים להשיג את מטרתם, וזאת למרות קיומם של חסמים ומערכי הגנה מסורתיים. לדוגמא, ארגון התקינה NERC (North American Electric Reliability Corporation), ממליץ לבצע הפרדה פיזית (Air-Gap) בין רשת ה-IT (Information Technology) לרשת ה-OT (Operation Technology) בארגונים בהם נעשה שימוש במערכות SCADA (Supervisory Control and Data Acquisition). עם זאת, באמצעות שימוש בהתקפת ערוץ צדדי ניתן 'לדלג' בין רשתות מבודדות, וזאת למרות קיומה של הפרדה פיזית. כפי שצוין לעיל, ניתן אף להשתמש בהתקפת ערוץ צדדי לשם הדלפת מפתחות הצפנה שכיחים, כדוגמת RSA[2], וזאת ללא יכולת ממשית של הארגון לזהות את דבר הדליפה (בהינתן כי הארגון מסתמך על מערכות הגנה מסורתיות).

אחת הדוגמאות הידועות בעולם אבטחת המידע להתקפת ערוץ צדדי, הינה התקפת 'HeartBleed', אשר כללה ניצול פגיעות ברכיבי תשתית SSL לשם הפקת מידע ערכי. להלן תיאור מקוצר של ההתקפה מויקיפדיה; "באפריל 2014 התגלתה ותוקנה פרצת אבטחה בגרסת OpenSSL 1.0.1 ו--OpenSSL 1.0.2 beta ובמספר גרסאות נוספות, שבה ניתן לחטוף עד 64KB של מידע רגיש מהשרת באמצעות תת-פרוטוקול הנקרא Heartbeat, שהוא פרוטוקול סינכרון. ההתקפה, הנקראת HeartBleed (פרפרזה על שם הפרוטוקול), מנצלת את העובדה שלא נעשית בדיקת גבולות (Bound Checking), בקשת סינכרון המכילה בית אחד והצבת הערך 65,536 בשדה המייצג את גודל ההודעה גורמת לשרת להפיק תגובה המכילה מידע מזיכרון היישום. אמנם התוקף אינו שולט בתוכנו אך גוש המידע עשוי להכיל אינפורמציה קריטית כמו עוגיות, סיסמאות ואף מפתח מאסטר של השרת."[3]

---

[2] לטובת תהליך ההצפנה, אלגוריתם RSA משתמש בחזקה (exponent)/"מעריך ציבורי", אשר ניתן 'לניחוש' באמצעות התקפת ערוץ צדדי (השוואת 'משתנה חיצוני' למודל חישובי מקביל). כמו כן, לשם שיפור ביצועי ההצפנה ופענוח, מערכות הצפנה שונות משתמשות ב'משפט השארית הסינית' (Chinese Remainder Theorem). עם זאת, ותלוי מימוש - השימוש ב'משפט השארית הסינית' עשוי להגדיל את מסגרת הפגיעות, וזאת לאור הסבירות לפגיעה באנטרופיה של תהליך ההצפנה.

[3] מקור: https://he.wikipedia.org/wiki/%D7%94%D7%AA%D7%A7%D7%A4%D7%AA_%D7%A2%D7%A8%D7%95%D7%A5_%D7%A6%D7%93%D7%93%D7%99, נדלה ב-14.12.2016.

ראוי לציין כי מעבר לנושא מיצוי מידע ערכי [4](פגיעה בסודיות המידע), ניתן להשתמש בהתקפת ערוץ צדדי לשם פגיעה בשלמות ו/או זמינות המידע ו/או מערכת המחשוב עצמה. עם זאת, בעיון בספרות המחקרית ניתן ללמוד כי קיימת התמקדות בנושא מיצוי מידע קריפטוגרפי ערכי ממערכות מחשוב באמצעות התקפה זו, וזאת לאור הקושי של גורמים שונים לפענח מידע ערכי אשר הוצפן באמצעות הצפנה סטנדרטית.

אקדים את המאוחר ואציין כי אין מאמר זה מתיימר להציג את כל עולם התוכן בנושא, וכי על מנת לפשט את המאמר בוצעו מספר הכללות, ובכלל זה יתכן כי יופיעו מספר אי דיוקים מסוימים בין המופיע בספרות המחקרית לבין הכתוב במאמר.

לסיכום חלק זה אציין כי המאמר מתמקד בהצגת מבוא ראשוני לנושא התקפת ערוץ צדדי, וזאת תוך שימוש בדוגמאות שכיחות מתחום המחקר, וזאת במטרה להראות את הקלות היחסית לביצוע דלף מידע ממערכות מחשוב באמצעות התקפה זו.

מקורות מידע ('ערוצי צד') אפשריים למימוש התקיפה

להלן מצ"ב סקירה בסיסית למקורות המידע העיקריים[5] (הידועים אף בשם "ערוצי הצד" / ערוצי פלט / ערוצי איסוף מידע) למימוש התקפת ערוץ צדדי:

א. מידע תיזמון (Timing):

מטבע הדברים, לשם השלמת פעולה חישובית נדרשת מסגרת זמן (Execution Time[6]), אשר ניתנת למדידה. קרי, בהינתן קלט מסוים, ביחס למערכת מחשוב מסוימת ואלגוריתם מסוים אשר נעשה בו שימוש, ישנה מסגרת זמן קבועה לביצוע כל פעולה חישובית, אשר ניתנת לעיתים קרובות למדידה על סמך פלט 'חיצוני'. תוקף אשר מודע לפרמטרים, כדוגמת אלגוריתם ההצפנה וארכיטקטורת המעבד אשר נעשה בהם שימוש[7], יכול לבנות מודל תיאורטי לתהליך החישוב, ולהשוות את המודל למסגרת הזמן אשר נמדדה באופן אמפירי מול הפלט 'החיצוני', ובכך למצות את קלט המקור לדוגמא.

---

[4] מידוע ערכי עשוי לכלול בין השאר, פרטי מידע העונים להגדרות הבאות: PHI (Protected Health Information), PII (Personally Identifiable Information), IP (Intellectual Property), Payment Details, Classified Information

[5] ניתן למצוא בספרות המחקרית חלוקה מגוונת של מקורות המידע העיקריים, דבר אשר עשוי לכלול שימוש במונחים שונים במקצת מהמונחים בהם נעשה שימוש במאמר זה.

[6] מונחים חלופיים באנגלית: Run time (Program Lifecycle Phase)

[7] ברמה התיאורטית אין חובה על התוקף לדעת פרמטרים אלו לשם מימוש ההתקפה. עם זאת, על מנת להפוך ההתקפה לישימה בפועל, סביר להניח כי התוקף ינסה לאסוף מידע מקדים על מערכת ההצפנה, דבר אשר עשוי לקצר את זמן ההתקפה בפועל.

להלן תרשים לדוגמא המציג תהליך הצפנה מסורתי, אשר כולל בין השאר; טקסט ללא הצפנה (Clear Text), מפתח הצפנה (Secret Key), אלגוריתם הצפנה (Encryption Algorithm) וטקסט מוצפן (Cypher Text):

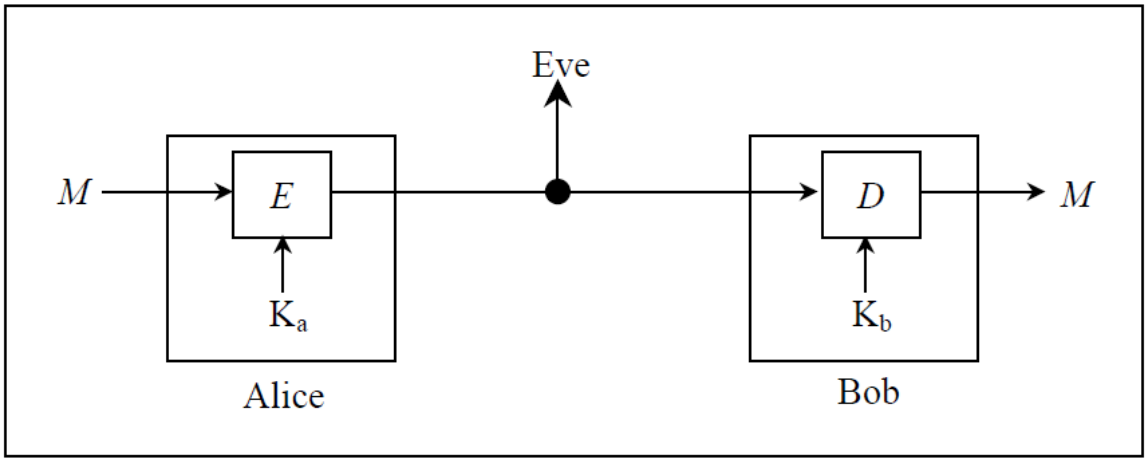


Figure 1: The traditional cryptographic model

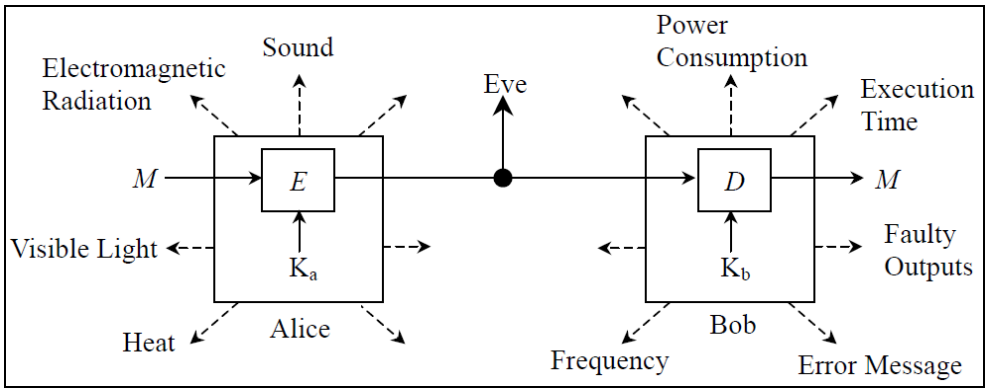
[8]

ההנחה המסורתית גרסה כי לאור העובדה כי תהליך ההצפנה והפענוח מתבצע בקופסה שחורה (Black Box), התוקף לא יוכל למצות את טקסט המקור (Clear Text), אף אם הוא ישיג העתק של הטקסט המוצפן (Cipher Text), ובכך הסוד יישאר מוגן.

עם זאת, ההנחה המסורתית התעלמה מהעובדה כי מערכת המחשוב פועלת באינטגרציה מול הסביבה, דבר אשר כולל תהליכי קלט ופלט מגוונים. כפי שצוין לעיל, התקפת ערוץ צדדי מתבססת על עקרון זה, כאשר במקרה של התקפת ערוץ צדדי מבוססת תיזמון (Timing Based Attack), התוקף משווה את הפלט 'החיצוני' המעיד על מסגרת הזמן אשר נדרשה לשם ביצוע פעולה חישובית במערכת המחשוב פלונית, לבין פלט מודל תיאורטי אשר בנה, ובכך הוא שואף להשיג חזקה על קלט מקור (הסוד).

[8] מקור: Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testi, YongBin Zhou, DengGuo Feng, State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences

להלן תרשים לדוגמא המציג את מקורות המידע (הידועים אף בשם 'ערוצי הצד' / ערוצי פלט / ערוצי איסוף מידע) השכיחים למימוש התקפת ערוץ צדדי, כאשר אחד מהם הינו ה"תיזמון" (Timing):



[9]

יוער כי התקפת ערוץ צדדי מבוססת תיזמון (Timing Based Attack) על אלגוריתמי הצפנה שכיחים (כדוגמת Diffie-Hellman, RSA, DSS) פורסמה במקור על ידי Paul C. Kocher בשנת 1996.

דוגמא אחרת להתקפת ערוץ צדדי מבוססת תיזמון (Timing Based Attack); שימוש ב- Blind SQL Injection ובחינת זמן התגובה (Response Time) של מערכת מחשוב היעד (כדוגמת משך הזמן אשר לוקח לשרת Web לספק מענה לשאילתת Select), וזאת תוך מיפוי ערכי אמת (Positive) ושקר (False), ביחס לטבלת ערכים מוגדרים מראש (כדוגמת טבלה המכילה רשימת Usernames פוטנציאליים). יצוין כי הנחת המוצא של התוקף הינה שזמן התגובה (Response Time) לערך אמת (Positive), יהיה שונה מזמן התגובה (Response Time) במקרה של ערך שקרי (False). יצוין כי מימוש התקפה זו הודגם כבר בשנת 2008 במסגרת כנס DEFCON 16. להלן מצ"ב הפנייה לסקירה מפורטת על התקפה זו: Time-Based Blind SQL Injection using Heavy Queries.

במאמר מוסגר, תוקפים רבים עושים שימוש בהתקפה המבוססת על מידע תיזמון (Timing) לטובת זיהוי ומעקף "קופסת חול" (Sandbox), וזאת אף ללא צורך בהתקנת כלי עזר ו/או הפעלת כלי עזר מובנה במערכת המחשוב המותקפת. דוגמא שכיחה להתקפה מסוג זו מבוססת על ניצול ה-Cache של הדפדפן (Browser) לרעה, וזאת באמצעות קוד גאווה סקריפט (Java Script) עוין המופעל מאתר האינטרנט של התוקף, דבר המאפשר לתוקף לקבל גישה למידע ערכי ממחשב הגולש[10].

[9] מקור: Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testi, YongBin Zhou, DengGuo Feng, State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences

[10] מקור: The Spy in the Sandbox: Practical Cache Attacks in JavaScript and their Implication, Yossef Oren, Vasileios P. Kemerlis, Simha Sethuma dhavan,Angelos D. Keromytis, Department of Computer Science, Columbia University, נדלה ב-17.12.2016

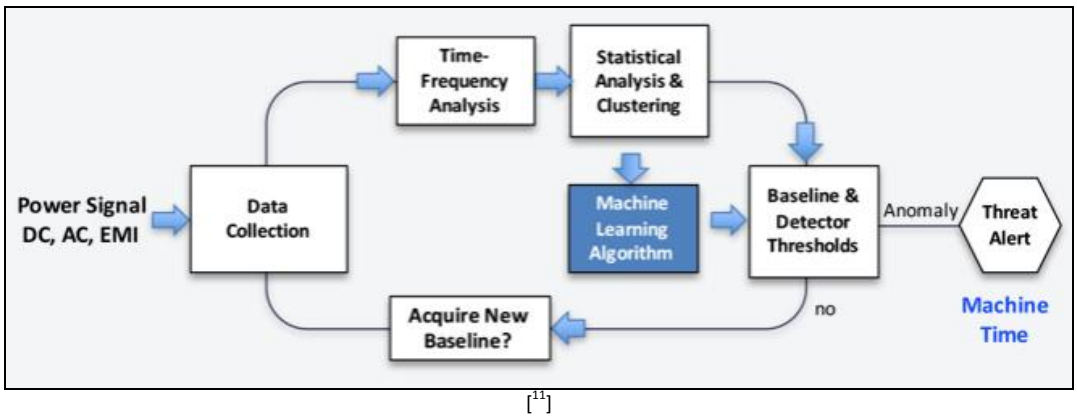
ב. צריכת אנרגיה (Energy Consumption):

ניתן לממש התקפה זו במספר אופנים לדוגמא; הראשון, לשם ביצוע פעולות חישוביות במערכת מחשוב, נדרש לוודא את קיומו של מקור אנרגיה (Energy Source) להזנת מערכת המחשוב. כפי שחברת חשמל (לדוגמא) יכולה לבחון את צריכת החשמל ברגע נתון בדירה פלונית, תוקף עשוי לבחון את צריכת החשמל של מערכת מחשוב פלונית (בהינתן כי אין למערכת המחשוב מייצב מתח עצמאי, אשר שומר על רמת צריכה קבועה), ולהסיק משינויי צריכת החשמל ובהקבלה למודל מתמטי מתאים, את מהות הפעולה החישובית המתבצעת בזמן נתון.

השני, על סמך שחלוף אנרגיה בין מערכת המחשוב לסביבה. שחלוף האנרגיה עשוי להיות חיובי (קליטת חום מהסביבה לדוגמא) או שלילי (פליטת חום לסביבה לדוגמא). גם במקרה זה ניתן לבצע בחינה של משתנה 'חיצוני' כדוגמת טמפרטורת הסביבה הקרובה למערכת המחשוב, ולהסיק משינויי טמפרטורת הסביבה ובהקבלה למודל מתמטי מתאים, את מהות הפעולה החישובית המתבצעת בזמן נתון. כמו כן, ישנם משתנים 'חיצוניים' נוספים הניתנים למדידה, וזאת כדוגמת רף האנרגיה הנפלט לסביבה ומביא לידי חימום\קירור במסגרת זמן נתונה (ב-BTU או ג'ול), והשינויים בלחץ אטמוספרי (ב-פסקל או PSI) במסגרת זמן נתונה (אם כי השינויים בלחץ הברומטרי בד"כ מינוריים יחסית, ולפיכך שימוש במשתנה 'חיצוני' זה אינו אפקטיבי דיו במרבית המקרים).

במאמר מוסגר, ניתן לראות כי חלק מפתרונות ההגנה על תשתית IoT (Internet of Things) ו-SCADA (Supervisory Control and Data Acquisition), מתבססים על בחינת מסגרת צריכת האנרגיה של מערכת המחשוב היעד לאורך זמן, וזאת לשם איתור אנומליה, אשר בתורה עשויה להעיד על קיומה של התקפה.

להלן תרשים סכמתי למנגנון הפעולה של פתרון איתור התקפה על תשתית IoT (Internet of Things) מבית PFP Cybersecurity:



[11]

[11] מקור: http://www.pfpcybersecurity.com/index.html

ג. דלף אלקטרומגנטי (Electromagnetic Leakage):

"קרינה אלקטרומגנטית (נקראת גם: קרינה א"מ או קרינה אלמ"ג) היא הפרעה מחזורית הרמונית בשדה החשמלי והמגנטי, המתפשטת במרחב. הפרעה כזו נקראת גל אלקטרומגנטי. חזית הגל של הקרינה האלקטרומגנטית מתקדמת בריק במהירות קבועה, שהיא מהירות האור בריק.[12]"

ניתן לממש התקפה זו במספר אופנים לדוגמא; הראשון, מערכת מחשוב מטבעה פולטת קרינה אלקטרומגנטית לסביבה[13], דבר אשר מאפשר לתוקף לבחון את השינויים בקרינה האלקטרומגנטית (תדירות הנמדדת ביחידות Hz או עוצמת גל - צפיפות ההספק של הגל, הנמדדת ביחידות של מיליוואט לסמ"ר mW/cm), ובהקבלה למודל מתמטי מתאים, להסיק מהי הפעולה החישובית המתבצעת בזמן נתון.

השני, עקב אופי ההשראה האלקטרומגנטית, ניתן לבצע בידול בין שתי שיחות (לדוגמא) הנישאות על אותו מדיום פיזי-תקשורתי בתדרים שונים, ובכך לבצע דלף מידע, וזאת ללא ידיעת הצדדים לשיחה.

השימוש הראשון אשר פורסם וכלל השימוש בדלף אלקטרומגנטי (Electromagnetic Leakage) למטרות מודיעין (Intelligence) נעשה כבר בשנות ה-50 של המאה הקודמת, ובהתאם לפרסומים שונים, ממשלת ארה"ב פיתחה מסגרת (Framework) בשם TEMPEST לטובת התקפה והתמודדות מול איום זה[14].

בשנת 2015 "חוקרים מאוניברסיטת תל אביב ומהטכניון (ד"ר ערן טרומר, חבר סגל במחלקה למדעי המחשב באוניברסיטת תל אביב; דניאל גנקין, דוקטורנט במחלקה למדעי המחשב בטכניון בהנחיה משותפת של ד"ר ערן טרומר (תל אביב) ופרופ' יובל ישי (טכניון); ולב פחמנוב ואיתמר פיפמן, מסטרנטים במחלקה למדעי המחשב באוניברסיטת תל אביב בהנחיה של ד"ר ערן טרומר) פיתחו שיטה לפיצוח צפנים המבוססת על הקשבה לשדה האלקטרומגנטי של המחשב[15]". הסבר פרטני על השיטה בה החוקרים השתמשו זמין בלינק הבא. יוער כי בהתאם לפרסומים השונים, הסיבה שבה החוקרים בחרו להתמקד בצפנים כיעד מחקר נבעה מזמן העיבוד הארוך של תהליך ההצפנה, דבר אשר אפשר איסוף נוח של פלט הקרינה האלקטרומגנטית. כמו כן, הדגמת יכולת זו בעלת חשיבות לעולם אבטחת המידע, וזאת מכיוון שישנו קושי מהותי לתוקפים לפענח את טקסט המקור (Clear Text) לאחר השלמת תהליך ההצפנה.

---

[12] מקור: https://he.wikipedia.org/wiki/%D7%A7%D7%A8%D7%99%D7%A0%D7%94_%D7%90%D7%9C%D7%A7%D7%98%D7%A8%D7%95%D7%9E%D7%92%D7%A0%D7%98%D7%99%D7%AA, נדלה ב-16.12.2016

[13] פרקטית מערכת מחשוב אף קולטת אלמ"ג מהסביבה, אך לשם פישוט המסגרת הדיונית, ואף לאור העובדה כי קליטת האלמ"ג נמוכה יחסית במקרה של מערכת מחשוב בדידה, אין מאמר זה כולל התייחסות לנושא זה.

[14] מקור: An Introduction to TEMPEST, SANS Institute InfoSec Reading Room

[15] מקור: כך תפרצו למחשב הנייד של השכן שלכם בעזרת פיתה, רדיו, וסמארטפון, ירון כהן צמח, דה מרקר, 26.06.2015, נדלה ב-17.12.2016

ד. מידע אקוסטי (Acoustic information):

"אקוסטיקה הוא ענף בפיזיקה העוסק בחקר הקול, גלים מכניים בגזים, נוזלים ומוצקים."[16] באמצעות ניצול תחום תוכן זה, תוקף עשוי לממש התקפה במספר אופנים; הראשון, מרבית מערכות המחשוב כוללות בחובן רכיבים המפיקים קול לסביבה, לדוגמא. מאוורר הקירור של יחידת עיבוד המרכזית (Central Processing Unit) עשויה לפלוט קול אשר עוצמתו ומשכו משתנה, וזאת בהתאם לעומס העבודה של מערכת המחשוב. סוגיה זו אף נכונה לגבי רכיבים מכניים נוספים במערכת המחשוב, לרבות רטט מארז האחסון והקלקה של משתמש על גבי המקלדת.

השני, רכיבים מכניים עשויים לגרום לשינוי ב'משטר הרוחות' (מלשון רוח) בסביבת מערכת המחשוב, דבר אשר ניתן למדידה באמצעים שונים. עם זאת, לא הצלחתי לאתר מחקר המציג מימוש מוצלח של אופן התקפה זה.

השלישי, מערכות מחשוב רבות מכילות אמצעי שמע, כדוגמת רמקולים, אוזניות. מטבע הדברים, אמצעי השמע פולטים לסביבה קול באופן רצוני (כדוגמת שמיעת מוזיקה ע"י המשתמש), ובאופן לא רצוני (כתוצאה מאינטגרציות חשמליות-פנימיות, אשר באות לידי ביטוי חיצוני כ"קול").

רביעית, בשנת 2013 הציגו פרופ' עדי שמיר, ד"ר ערן טרומר והדוקטורנט דניאל גנקין עבודת מחקר אשר הדגימה יכולת לביצוע הדלפת מפתחות הצפנה (כדוגמת RSA)[17], וזאת על סמך איסוף אותות אקוסטיים אשר מקורם מרעידת רכיבים אלקטרוניים בהם מועבר זרם חשמלי, כאשר רכיבים אלו מנסים לשמור על אספקה קבועה של זרם ליחידת העיבוד המרכזית (Central Processing Unit), וזאת למרות תנודות בצריכת האנרגיה אשר נגרמות כתוצאה מביצוע פעולות חישוב.

האופנים אשר צוינו לעיל מאפשרים מדידה של המשתנים 'החיצוניים', דבר אשר מאפשר לתוקף לבחון את השינויים באותם משתנים ובהקבלה למודל מתמטי מתאים, להסיק מהי הפעולה החישובית המתבצעת בזמן נתון.

חמישית, הודגמו מספר מקרים שבהם חוקרים, כדוגמת החוקר הראשי מרדכי גורי ממרכז המחקר לאבטחת סייבר (CSRC) של אוניברסיטת בן-גוריון בנגב, ניצלו פעילות Malware במערכת מחשוב[18], וזאת במטרה להפוך את מערכת המחשוב למעין 'משדר', אשר אפשר להם להדליף מידע בין רשתות נפרדות

---

[16] מקור: https://he.wikipedia.org/wiki/%D7%90%D7%A7%D7%95%D7%A1%D7%98%D7%99%D7%A7%D7%94, נדלה ב-16.12.2016

[17] מקור: פרופ' עדי שמיר פיתח שיטה לפריצת הצפנה על ידי האזנה למחשב, עומר כביר, כלכליסט, 22.12.2013, נדלה ב-16.12.2016.

[18] מקור: Fansmitter: Acoustic Data Exfiltration from (Speakerless) Air-Gapped Compute, Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, Yuval Elovici Ben-Gurion University of the Negev Cyber Security Research Center

פיזית (Air-Gap), כאשר המקלט היה מחובר לרשת היעד. יוער בחלק מן המחקרים נעשה שימוש בפורמט מידע בינארי, כאשר תדר צליל X (הרץ) זוהה כ-"0", ואילו תדר Y (הרץ) זוהה כ-"1". לחילופין, נעשה שימוש דומה בעוצמת קול, כאשר עוצמת צליל X (דציבל) זוהתה כ-"0", ואילו עוצמת צליל Y (דציבל) זוהתה כ-"1".

במאמר מוסגר, ישנן שיטות נוספות לקידוד מידע אקוסטי בעת העברתו במדיומים שונים, אך קצרה היריעה מלסקור את שיטות אלו במאמר זה.

ה. השתיירות מידע (Data Remanence or Electromagnetic Emanations):

"מחיקה מלאה של נתונים או מחיקת מידע לצמיתות (באנגלית Data erasure או Data wiping) היא פעולה של מחיקת נתונים דיגיטליים באופן שלא יהיה ניתן לשחזרם. את הפעולה אפשר לבצע על גבי דיסק קשיח או מדיה דיגיטלית אחרת. בשונה ממחיקת נתונים רגילה, שרק "מתעלמת" מעצם קיומם של הנתונים, מחיקת נתונים לצמיתות מוחקת את כל הנתונים על המדיה תוך השארת הדיסק מפורמט. התקני מדיה חדשים מבוססי פלאש כגון: דיסק און קי, דיסק SSD, וכרטיסי SD יכולים לגרום לטכניקות מחיקת הנתונים להיכשל ולאפשר שחזור של הנתונים למרות הפעולות שננקטו למחיקת הנתונים לצמיתות."[19]

בהתאם, ניתן לזהות מקרים רבים בהם מידע שיורי ניתן למיצוי מיחידת האחסון, וזאת למשך תקופה שאורכה משתנה, ותלוי בסוג יחידת התקן האחסון ושיטת המחיקה בה נעשה שימוש במקור. שיטת מיצוי זו עשויה לכלול איסוף מידע באופן פאסיבי (כדוגמת מדידת רמת מגנטיות של יחידת האחסון - ביחידות ובר והשוואתה לתוצר צפוי) או שיטות אקטיביות (כדוגמת יצירת שדה חשמלי סביב יחידת האחסון, ובחינת ההבדלים בין 'מצב אפס', למצב אקטיבי. יחידות מדידה ניוטון לקולון או וולט למטר).

ו. פליטת פוטונים (Photonic Emissions)

בהתאם לויקיפדיה; "הפוֹטוֹן (באנגלית: Photon) הוא החלקיק היסודי המייצג מנה (קוונטום) של אור, הנושא את הכוח האלקטרומגנטי. הוא אחראי לתופעות הקרינה האלקטרומגנטית השונות בכל אורכי הגל, ובכללן מגוון רחב של תופעות פיזיקליות הכוללות את צבעי האור הנראה, שידורי רדיו, קרני רנטגן, וכדומה.

[19] מקור: https://he.wikipedia.org/wiki/%D7%9E%D7%97%D7%99%D7%A7%D7%94_%D7%9E%D7%9C%D7%90%D7%94_%D7%A9%D7%9C_%D7%A0%D7%AA%D7%95%D7%A0%D7%99%D7%9D, נדלה ב-17.12.2016

לפוטון, כמו לחלקיקים אחרים, ישנן תכונות הן של גל והן של חלקיק, תופעה הנקראת "דואליות גל-חלקיק". התופעות דמויות-גל שמציגים הפוטונים, הן לדוגמה שבירה על ידי עדשה והתאבכות. התכונות החלקיקיות של הפוטון הן, בין השאר, פיזור והעברת אנרגיה במנות בדידות. פוטון שעובר אינטראקציה מלאה עם אטום או עם מולקולה נבלע ומוסר (או נפלט ומקבל) את כל האנרגיה שלו תוך כך. בעקבות האינטראקציה, עוברים האטום או המולקולה עירור או יינון. עבור אור בתחום הנראה, האנרגיה הנישאת על ידי פוטון יחיד היא כ 4×10-19-ג'ול, כמות אנרגיה המספיקה לעורר מולקולה יחידה של תא קולט אור בעין, וליצור בכך אות עצבי שהוא הבסיס הפיזיולוגי לראייה. לפוטונים ישנן אינטראקציות נוספות עם החומר, כאפקט קומפטון, בו משנה הפוטון את אנרגייתו ולכן גם את אורך הגל, ויצירת זוג, שבה אלקטרון ופוזיטרון נוצרים מפוטון בודד העובר ליד אטום כבד. פוטונים יכולים להיפלט מגרעין אטום לא יציב בצורת קרינת גמא, וכמו כן הם יכולים להיפלט על ידי חלקיקים טעונים הנמצאים בתאוצה.

באלקטרודינמיקה קוונטית, הפוטון יכול לשמש כמתווך בתהליכים אלקטרומגנטיים, כלומר, האינטראקציה מתרחשת באמצעות החלפת פוטונים בין חלקיקים טעונים. למעשה, כל השדות החשמליים והמגנטיים ניתנים לתיאור באמצעות פוטונים. לפי המודל הסטנדרטי של פיזיקת החלקיקים, קיום הפוטון הוא תוצאה של הדרישה כי לחוקים הפיזיקליים תהיה סימטריה מסוימת בכל נקודה במרחב-זמן. תכונות הפוטונים, כגון מטען חשמלי, מסה וספין, נקבעות על ידי מאפייני סימטריה זו (סימטריית כיול).

הרעיון כי האור נישא במנות בדידות, כלומר באמצעות פוטונים, פותח על ידי אלברט איינשטיין החל משנת 1905. איינשטיין נתן פירוש לנוסחה שאותה הציע מקס פלאנק על-מנת להסביר את הספקטרום של קרינת גוף שחור: [2]. איינשטיין זיהה את E עם אנרגיית קוונט אחד של קרינה אלקטרומגנטית, שלימים נקרא פוטון, ואת עם התדירות של הקרינה. באמצעות מודל הפוטונים הצליח איינשטיין להסביר את האפקט הפוטואלקטרי, ויחד עם הפיזיקאי ההודי סאטינדרה נאת בוז הוא סיפק תיאור סטטיסטי של אור המסביר את קרינת פלאנק. בנוסף, מתוך שיקולים סטטיסטיים, הסיק איינשטיין את קיומו של מנגנון הפליטה המאולצת וכן מצא קשרים בין מקדמי הבליעה והפליטה של אור על ידי חומר.

גילוי מודל הפוטון הביא לפריצות דרך בפיזיקה הניסויית והתאורטית, כגון פיתוח הלייזרים, יצירת עיבוי בוז-איינשטיין ובאופן כללי הביא להתפתחות מכניקת הקוונטים. תחומים רבים אחרים התקדמו בזכות הבנת מושג הפוטון, כמו למשל פוטוכימיה, מיקרוסקופיה בהפרדה גבוהה ומדידת מרחקים ברמה המולקולרית. לאחרונה נמצא שימוש ישיר במושג הפוטון במחקרים העוסקים במחשוב קוונטי וביישומי תקשורת אופטית מתקדמים, כגון הצפנה קוונטית.[20]"

[20] מקור: https://he.wikipedia.org/wiki/%D7%A4%D7%95%D7%98%D7%95%D7%9F, נדלה ב-18.12.2016

בדומה לאלקטרומגנטיות, ניתן למדוד את פליטת ו/או בליעת הפוטונים במערכת מחשוב ו/או בסביבתה בזמן נתון, ובכך להשיג מקור מידע נוסף אשר מאפשר לתוקף לבחון את השינויים במשתנים 'חיצוניים' אלו, ובהקבלה למודל מתמטי מתאים, להסיק מהי הפעולה החישובית או פעולה אחרת (כדוגמת הצגת תמונה על מסך) המתבצעת בזמן נתון.

אחד מן היתרונות הבולטים בשימוש בפליטת פוטונים (Photonic Emissions) כמקור מידע הינה העובדה כי פליטת הפוטונים (Photonic Emissions) עשויה 'להשתקף' כאשר היא פוגעת בעצם (כדוגמת קיר), ולפיכך תוקף עדיין יכול לקבל מידע אשר ניתן להפיק ממנו מידע ערכי (אם כי הדבר בד"כ מחייב שימוש באלגוריתמים נוספים, לרבות 'תיקוני סטייה').

ז. שרשראות (ערוצי) סריקה (Scan Chains):

עיצוב לטובת בדיקה (Design for Testing[21]) הינו שם כולל לטכניקות אשר מטרתן להוסיף למעגלים משולבים (Integrated Circuit), הידועים בציבור בשם צ'יפים, תכונות (יכולות) אשר יוכלו לסייע בווידוא כי חומרת המעגלים המשולבים (Integrated Circuit) אשר יוצרה במפעל, אינה מכילה פגמים, אשר עשויים לפגוע בתפקוד הרצוי/המתוכנן. כמו כן, טכניקות אלו יכולות אף לסייע ליצרן בכימות ה-MTBF (Mean Time Between Failures) הצפוי של רכיבים בתנאי עבודה שונים.

שרשראות (ערוצי) סריקה (Scan Chains) הינה טכניקה שכיחה לבדיקת תקינות מעגלים משולבים (Integrated Circuit) מבוססי סיליקון, המבוססת על עקרונות עיצוב לטובת בדיקה (Design for Testing).להלן מספר מושגי יסוד אשר יסייעו בהמשך בהסברת אופן ההתקפה:

- **מעגל לוגי צירופי (Combinational Logic Circuit)** - הינו מעגל חשמלי שהפלט שלו הוא פונקציה של הקלט הנוכחי אשר התקבל. ברגע שקלט המקור משתנה, המידע על הקלט הקודם נמחק. כלומר, אין סוג מעגל חשמלי זה כולל בחובו יחידת אחסון זיכרון.
- **מעגל לוגי סדרתי (Sequential Logic Circuits)** - הינו מעגל חשמלי שהפלט שלו הוא פונקציה של הקלט מהעבר ו/או הנוכחי. מקובל כי מעגל לוגי סדרתי בנוי כמעגל לוגי צירופי, וזאת בתוספת יחידת אחסון זיכרון (לשמירת קלט מהעבר) ומנגנון משוב (Feedback). העיקרון המתמטי מבוסס על 'מכונה סדרתית' (Sequential Machine). ישנם שני מצבי עבודה מקובלים; מוד סינכרוני ('מצב יציב') - "פעולת המערכת מתבצעת ב"פיקודו" של שעון וערכי המערכת נקבעים מערכי הכניסה בנקודות זמן

[21] שם חלופי: Design For Testability

מסוימות שהינן תלויות שעון (מצב המערכת תלוי שעון)[22]". מוד אסינכרוני ('מצב מהיר') - "פעולות המערכת תלויות בסדר של שינוי הכניסות, מצב המערכת יכול להשתנות בכל רגע[23]".

כמו כן, יש לשים את הדעת כי ככל שהמעגל החשמלי מורכב יותר (מכיל יותר שערים לוגיים לדוגמא), זמן ההשהיה מרגע שינוי בקלט ועד להתייצבות הפלט על הערך הנכון הוא ארוך יותר.

- **אוגר הזזה (Shift Register)** - הינו אוגר (תא אחסון נתונים בצורת אוסף סיביות/ביטים, Bits) שבו ניתן להזיז את הנתונים הבינריים (האגורים בו) ימינה או שמאלה. אוגר הזזה בנוי מדלגלגים המחוברים זה לזה בטור, כך שמוצא דלגלג אחד משמש כמבוא הדלגלג הבא בשרשרת. כל הדלגלגים מחוברים לאותו 'אות שעון'. תפקיד אות השעון הוא לתזמן נכונה את הפעילות של רכיב אלקטרוני אחד או יותר, וזאת כדוגמת הזמן לביצוע הזזה אחת של הנתונים הבינריים המאוחסנים באוגר ההזזה (Shift Register). יוער כי הסיביות (Bits) אשר יוצאות מתחום האוגר "הולכות לאיבוד".

- **בריח/נועל (Latch)**[24] - הוא מעגל דו-יציב (מעגל אשר יכול לקבל מצב אחד מבין שני מצבים יציבים) שמסוגל לזכור סיבית (Bit) אחת. הפלט (Output) עשוי להשתנות בכל זמן נתון, וזאת בהתאם לשינוי בקלט (Input) (מערכת א-סינכרונית).

- **דלגלג/פליפ פלופ (Flipflops)** - עקרון הפעולה של רכיב זה דומה לבריח/נועל (Latch), אך במקרה זה הפלט (Output) תלוי בקיומו של סיגנל (כדוגמת 'אות שעון'), המתזמן את המופע ביחס לקלט (Input).

במהלך הבדיקה, הבודק עשוי לגרום לשינוי במצב הדלגלג/פליפ פלופ (Flipflops) ו/או הנועלים (Latch), דבר אשר גורם להיסט של הנתונים הבינאריים המאוחסנים באוגר ההזזה (Shift Register). עקב כך, המעגל הלוגי צירופי (Combinational Logic Circuit) הרלוונטי מומר באופן זמני למעין מעגל לוגי צירופי (Combinational Logic Circuit), דבר המאפשר לבודק להשוות את הפלט בפועל ביחס לפלט המצופה.

על מנת לאפשר בפועל את ביצוע הבדיקה, יצרן המעגלים המשולבים (Integrated Circuit) מוסיף כבר בשלב התכנון נקודות מבחן (Test Points Insertion) למעגל החשמלי, אשר מטרתן להקל על ביצוע הבדיקה.

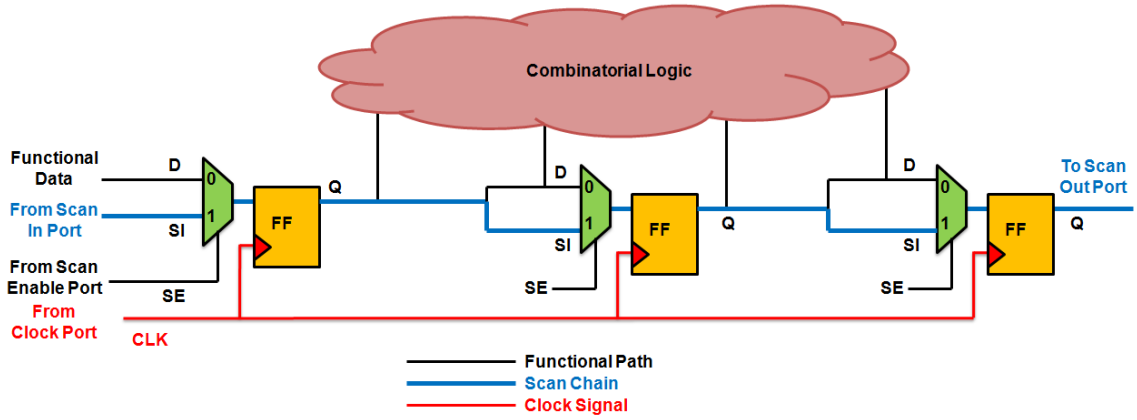
---

[22] מקור: Flip Flop, יהודה אפק, נתן אינטרטור, אוניברסיטת תל אביב

[23] שם.

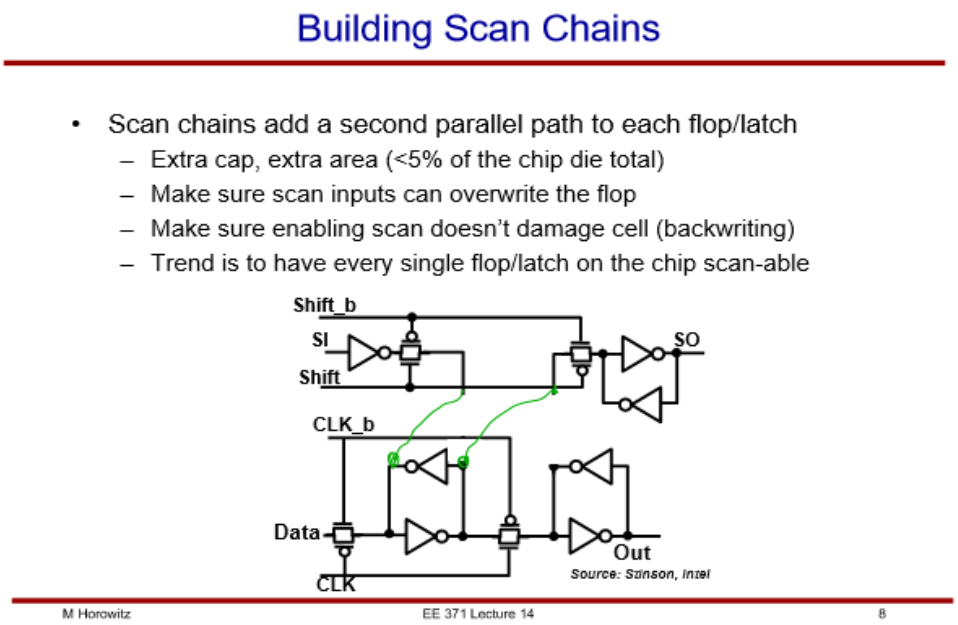
[24] ההבדל בין דלגלג/פליפ פלופ (Flipflops) לבריח/נועל (Latch) "מטושטש" כיום, וזאת לאור העובדה כי בפסי הייצור בד"כ מייצרים דלגלג/פליפ פלופ (Flipflops), ולאחר מכן מתכנן המעגל החשמלי מחליט האם לאפשר את קיומו של סיגנל (כדוגמת 'אות שעון'), או לא.

להלן מצ"ב תרשים לתיאור תהליך הבדיקה ברמת-על:



[25]

להלן דוגמא לקלות היחסית שבה ניתן ליצור ערוץ מקביל לדלגלים (Flipflops) ו/או הנועלים (Latch) הקיימים במעגל החשמלי, דבר המאפשר לגרום לשינוי לא רצוני בהתנהגות המעגל החשמלי:



[26]

למרות היתרונות הגלומים בטכניקה בדיקה זו, היא עשויה לאפשר לתוקף לקבל נגישות פיזית מתקדמת ל-SoC (System on a Chip) לדוגמא, ובכך להפיק מידע ערכי, כדוגמת ערכו של מפתח הצפנה מוטמע. יוער כי אין התוקף נדרש (בד"כ) לתקוף את שכבת התוכנה (כדוגמת מערכת ההפעלה) על מנת להשיג

[25] מקור: http://anysilicon.com/overview-and-dynamics-of-scan-testing/, נדלה ב-18.12.2016.

[26] מקור: Lecture 14 - Design for Testability, M. Horowitz, Computer Systems Laboratory, Stanford University

את מטרתו בעת שימוש בהתקפה זו, אלא די שהוא מצליח להתממשק כיאות לנקודות המבחן (Test Points Insertion) אשר היצרן הטמיע במקור, ולאחר מכן לבצע בדיקה דומה לזו אשר היצרן ביצע.

ח. הזרקת שגיאה (Faults Injected):

מאפייני התקפת ערוץ צדדי (Side-Channel Attack) על בסיס הזרקת שגיאה (Faults Injected) מזכירים ברמה מסוימת מאפייני תקיפת Buffer Overflow ברמת התוכנה. בהתקפה זו, התוקף גורם לתקלה נקודתית בחומרה (כדוגמת קיצור מעגל חשמלי, קפיצות מתח, שינוי זמן מערכת, שינוי טמפרטורת עבודה, שימוש בלייזר, שימוש בקרני רנטגן ויצירת גישור ישיר בין רכיבים שונים במעגל החשמלי), דבר הגורם לשינוי לא רצוני בהתנהגות הרכיב המותקף (פגיעה בשלמות התהליך/שיבוש). תוצאה שכיחה לתקיפה זו הינה היפוך (Flipflops) במצב הסיביות/ביטים (Bit) המאוחסנות ביחידת אחסון הזיכרון. בהתאם, באמצעות טכניקה זו התוקף יכול לזהות מידע ערכי על מערכת המחשוב, כדוגמת הלוגיקה הקיימת / סוגי האלגוריתמים בהם נעשה שימוש, ופרטי מפתח הצפנה המובנה במערכת.

ט. 'שורת הפטיש' (Row Hammer) / DRAM Bug:

התקפת 'שורת הפטיש' (Row Hammer) פורסמה בשנת 2014[27], ובהתאם לטענת החוקרים (Yoongu Kim,Ross Daly,Jeremie Kim, Chris Fallin, Ji Hye Lee, Donghyuk Lee, Chris Wilkerson, Konrad Lai, Onur Mutlu) היא מבוססת על כשל (באג) בתהליך הייצור של כרטיסי/מודולי DRAM (Dynamic Random-Access Memory), אשר ניתן לניצול לרעה.[28]

עקרון ההתקפה מבוסס על ביצוע פעולות כתיבה (Write) / קריאה (Read) / הרצה (Execute) תכופות בשורת (Raw) אחסון פלונית של כרטיס/מודול ה-DRAM, דבר אשר עשוי לגרום, לבסוף, לשינוי לא רצוני במצב הדלגלגים/פליפ פלופ (Flipflops) הקיימים בשורות (Rows) אחסון צמודות ('שכנות').

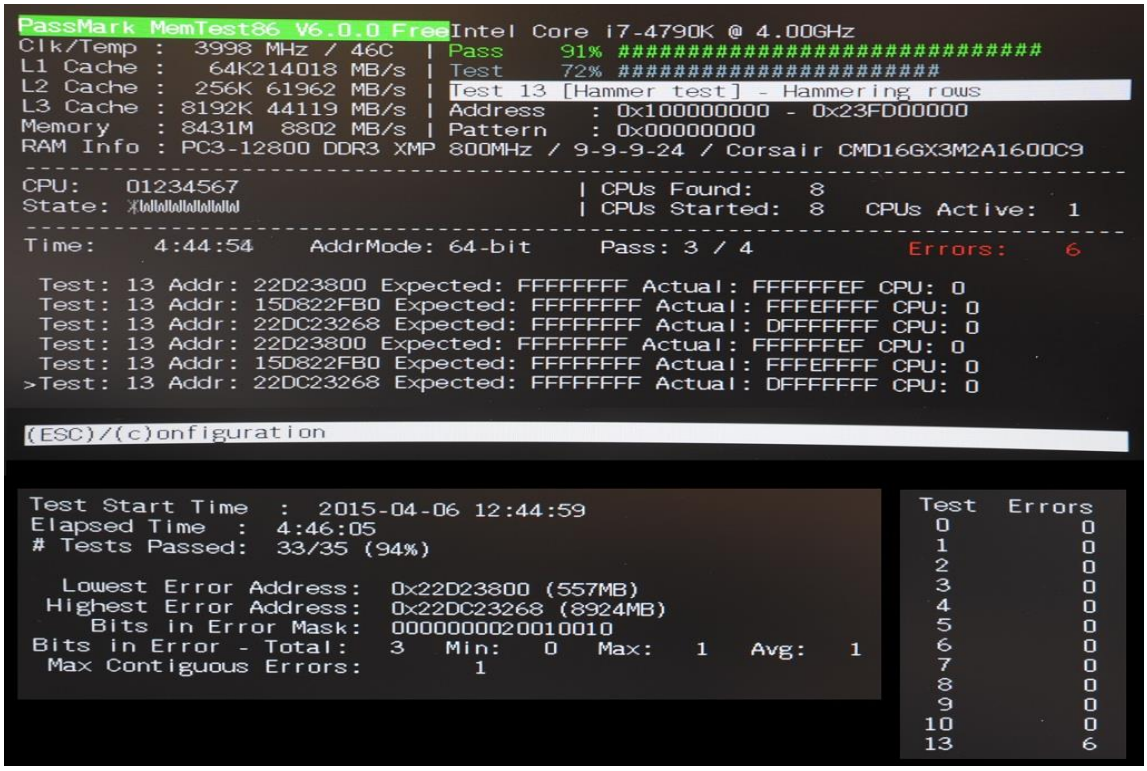
באמצעות התקפה זו, תוקף עשוי לקבל נגישות אשר תאפשר לו לנצל תהליך פלוני (Process) לשם השפעה על תהליך (Process) אלמוני. ובכך, התוקף עשוי לקבל לבסוף הרשאות יתר (Privilege Escalation), כאשר במקביל מנגנוני ההגנה השכיחים לניהול זיכרון אינם 'מודעים' כלל לקיומה של ההתקפה. יוער כי סוג התקפה זה שכיח בעת ניסיון לעקיפת רכיבי הגנה מבוססי 'קופסת חול' (Sandbox).

---

[27] מקור: Exploiting the DRAM rowhammer bug to gain kernel privileges, Mark Seaborn, sandbox builder and breaker, with contributions by Thomas Dullien, reverse engineer

[28] מקור: Flipping Bits in Memory Without Accessing Them: An Experimental Study of DRAM Disturbance Error, Yoongu Kim,Ross Daly,Jeremie Kim, Chris Fallin, Ji Hye Lee, Donghyuk Lee, Chris Wilkerson, Konrad Lai, Onur Mutlu, Carnegie Mellon University and Intel Lab

להלן דוגמא להמחשה לתוצאות בדיקה המאפשרת איתור פגיעות בכרטיס/מודולי זיכרון מבית חברת Corsair, אשר מהווה את הבסיס להצלחתה של התקפת 'שורת הפטיש' (Row Hammer):



[29]

י. שימוש במד-תאוצה (Accelerometer) המובנה בטלפון חכם (Smart Phone):

מד-התאוצה (Accelerometer) המובנה בטלפון חכם (Smart Phone) מהווה חיישן המאפשר למדוד תאוצה קווית. מד-התאוצה מספק לרוב וקטור, גודל וכיוון, של התאוצה אותה הוא חש בציר מסוים[30]. מטרת מד-התאוצה במרבית הטלפונים החכמים (Smart Phones) היא לייצב את מסך התצוגה והמצלמה. ההתקפה המבוססת על ניצול מד-התאוצה (Accelerometer) פורסמה בשנת 2011. בשלב הראשון של ההתקפה, התוקף מאתר באמצעות מד-התאוצה (Accelerometer) ויברציות (Vibration) אשר מקורן מהקלדת רצפי הקלדה סמוכים של צמד אותיות (ימין-שמאל לדוגמא) ממקלדת מחשב הנמצאת בסמיכות לטלפון חכם (Smart Phone). בשלב השני, התוקף משווה באופן סטטיסטי את המידע שקיבל למילים

[29] מקור: http://forum.corsair.com/v3/showthread.php?p=777033, נדלה ב-25.12.2016

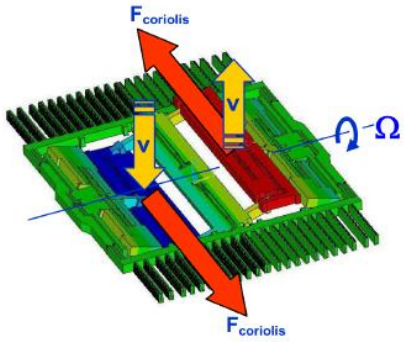
[30] מקור: https://he.wikipedia.org/wiki/%D7%9E%D7%93_%D7%AA%D7%90%D7%95%D7%A6%D7%94, נדלה ב-25.12.2016

מוכרות ממילון (Dictionary), ובכך הוא מסוגל לחשוף מידע ערכי אשר הוזן ע"י המשתמש. לטענת צוות החוקרים בראשות פרופ' Patrick Traynor, הם הגיעו לרמת הצלחה של כ-80 אחוזים[31].

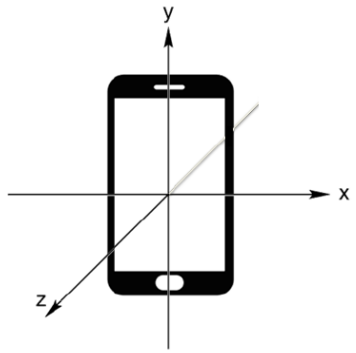
יא. שימוש בגירוסקופ (Gyroscope) המובנה בטלפון חכם (Smart Phone) בשילוב למידת מכונה:

"גירוסקופ או ג'יירוסקופ, נקרא לעתים ג'יירו בקיצור (באנגלית: Gyroscope, מיוונית "גירוס"="עיגול, סיבוב" ו"סקופוס"="ראייה"; השם הומצא על ידי הפיזיקאי הצרפתי לאון פוקו ב-1852) - הוא מכשיר מדעי המשמש למדידה או שמירה של יציבות, תוך התבססות על עקרונות שימור התנע הזוויתי. בפיזיקה, שם זה ידוע גם כאינרציה גירוסקופית. אחד השימושים הנפוצים של מכשיר זה הוא מדידת הזווית שבין גוף הנמצא בתנועה לגוף במצב אופקי, כאשר המצב האופקי בדרך כלל הוא הקרקע של כדור הארץ."[32]

שכיח לראות כיום כי מרבית הטלפונים החכמים (Smart Phones) מכילים גירוסקופ (Gyroscope) המבוסס על טכנולוגיית MEMS (Micro Electro Mechanical System). להלן דוגמא לעקרון הפעולה של גירוסקופ (Gyroscope) המבוסס על טכנולוגיית MEMS (Micro Electro Mechanical System) - השינוי הזוויתי גורם להשפעה ביחס המסה ('המטוטלת'), אשר ניתן להמירה לערך חישובי:



(b) Driving mass movement depending on the angular rate



[33] Figure 4: Coordinate system of Android and iOS.

החוקרים Yan Michalevsky, Dan Boneh, Gabi Nakibly הדגימו כי ניתן 'להסב' גירוסקופ (Gyroscope) המבוסס על טכנולוגיית MEMS (Micro Electro Mechanical System) למעין אמצעי האזנה (בדומה

[31] מקור: Researchers can keylog your PC using your iPhone's accelerometer, Chris Foresman, 2011, נדלה ב-25.12.2016

[32] מקור: https://he.wikipedia.org/wiki/%D7%92%D7%99%D7%A8%D7%95%D7%A1%D7%A7%D7%95%D7%A4, נדלה ב-29.12.2016

[33] מקור: Gyrophone: Recognizing Speech From Gyroscope Signals, Yan Michalevsky and Dan Boneh, Computer Science Department Stanford University, Gabi Nakibly, National Research & Simulation Center Rafael Ltd

למיקרופון)[34], וזאת באמצעות איסוף מידע על תנודות אקוסטיות בסביבת הטלפון החכם (Smart Phone). עם זאת, לאור העובדה כי טווח התדרים אשר ניתן לאיסוף באמצעות גירוסקופ (Gyroscope) אינו עולה על 200 Hz, כאשר התדירויות אשר אוזן האדם מסוגלת לשמוע נעה בטווח 20 Hz ל-20,000[35], החוקרים נאלצו להשתמש בשיטות תיקון ('השלמת תוכן') מבוססות Machine Learning (כדוגמת NLP[36]). כפועל יוצא מכך החוקרים הצליחו להפיק מידע ערכי, ואף להגביר את רמת ההצלחה באמצעות ביצוע איסוף מידע אקוסטי ממספר טלפונים החכמים (Smart Phones).

סיכום

התקפת ערוץ צדדי (Side-Channel Attack) אינה התקפה חדשה, אך למרות זאת, רבים בשוק אבטחת המידע אינם מודעים לקיומה, או לחילופין, רבים אינם מתייחסים אליה כמקור איום מהותי. עם זאת, המציאות מלמדת כי ניתן לממש את התקפה זו בשורה של וריאציות שונות ומגוונות, אשר השלכותיהן הרוחביות עשויות לאפשר לתוקף להשיג חזקה במערכת מחשוב קריטיות, ואף לפגוע בתהליכים עסקיים קריטיים בארגון. כמשפט לסיום אציין כי כנסי אבטחת מידע בינלאומיים, כדוגמת DEFCON 24 משנת 2016, מדגישים את חשיבות ההערכות המוקדמת של ארגונים להתמודדות עם איומים מסוג אלו.

> "There is a greater darkness than the one we fight. It is the darkness of the soul that has lost its way. The war we fight is not against powers and principalities, it is against chaos and despair. Greater than the death of flesh is the death of hope, the death of dreams. Against this peril we can never surrender. The future is all around us, waiting in moments of transition, to be born in moments of revelation. No one knows the shape of that future, or where it will take us. We know only that it is always born in pain."
>
> - Book of G'Quan

[34] מקור: Gyrophone: Recognizing Speech From Gyroscope Signals, Yan Michalevsky and Dan Boneh, Computer Science Department Stanford University, Gabi Nakibly, National Research & Simulation Center Rafael Ltd.

[35] מקור: http://hypertextbook.com/facts/2003/ChrisDAmbrose.shtml, נדלה ב-29.12.2016

[36] Natural Language Processing

על המחבר

יובל סיני הינו מומחה אבטחת מידע, סייבר, מובייל ואינטרנט, חבר קבוצת SWGDE של משרד המשפטים האמריקאי. כמו כן, יובל סיני קיבל הכרה מחברת Microsoft העולמית כ-MVP בתחום Enterprise Security.

מילות מפתח

Acoustic information, Air-Gap, Compare Cryptanalysis, Cryptographic Attacks, Data Remanence, Design for Testability, DFT, Electromagnetic Emanations, Electromagnetic Leakage, Energy Consumption, Faults Injected, Hardware Threat Model, Photonic Emissions, Scan Chains, Side-Channel Attack, Root of Trust, TEMPEST, Timing

ביבליוגרפיה

ביבליוגרפיה באנגלית:

מאמרים:

- Exploiting the DRAM rowhammer bug to gain kernel privileges, Mark Seaborn, sandbox builder and breaker, with contributions by Thomas Dullien, reverse engineer
- USBee: Air-Gap Covert-Channel via Electromagnetic Emission from USB, Mordechai Guri, Matan Monitz, Yuval Elovici, Cyber Security Research Center, Ben-Gurion University of the Negev, 2016
- Gyrophone: Recognizing Speech From Gyroscope Signals, Yan Michalevsky and Dan Boneh, Computer Science Department Stanford University, Gabi Nakibly, National Research & Simulation Center Rafael Ltd.
- Physical Key Extraction Attacks on PCs, Daniel Genkin, Lev Pachmanov, Itamar Pipman, Adi Shamir, Eran Tromer, Communications of the ACM, Vol. 59 No. 6, Pages 70-79, 2016
- Fansmitter: Acoustic Data Exfiltration from (Speakerless) Air-Gapped Compute, Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, Yuval Elovici Ben-Gurion University of the Negev Cyber Security Research Center

- Stealing Keys from PCs using a Radio: Cheap Electromagnetic Attacks on Windowed Exponentiation, Daniel Genkin, Lev Pachmanov, Itamar Pipman and Eran Tromer, Tel Aviv University, March 2, 2015
- Quadrennial Technology Review 2015, Cyber and Physical Security, Chapter 3: Technology Assessment, U.S. Deprtment of Energy
- Frequency Range of Human Hearing, Glenn Elert
- 8 Technologies That Can Hack Into Your Offline Computer and Phone, Farzan Hussain, 2015
- Stealing Data From Computers Using Heat
- Blog: Testing for Row Hammer
- Unconditionally Secure Quantum Signatures, Ryan Amiri and Erika Andersson, Entropy 2015, 17, 5635-5659
- Flipping Bits in Memory Without Accessing Them: An Experimental Study of DRAM Disturbance Error, Yoongu Kim, Ross Daly, Jeremie Kim, Chris Fallin, Ji Hye Lee, Donghyuk Lee, Chris Wilkerson, Konrad Lai, Onur Mutlu, Carnegie Mellon University and Intel Lab
- Functional Scan Chain Testing, Douglas Chang, CS Department and Kwang-Ting Cheng and Malgorzata Marek-Sadowska, ECE Department, University of California, and Mike Tien-Chien Lee, Avant! Corp
- Overview and Dynamics of Scan Chain Testing
- Breaking the Sandbox, Sudeep Singh
- The Spy in the Sandbox: Practical Cache Attacks in JavaScript and their Implication, Yossef Oren, Vasileios P. Kemerlis, Simha Sethuma dhavan, Angelos D. Keromytis, Department of Computer Science, Columbia University
- Data Remanence in Semiconductor Devices, Peter Gutmann, IBM T.J.Watson Research Center
- An Introduction to TEMPEST, SANS Institute InfoSec Reading Room
- ASSESSMENT AND TESTING OF INDUSTRIAL DEVICES ROBUSTNESS AGAINST CYBER SECURITY ATTACKS, F. Tilaro, B. Copy, CERN, Geneva, Switzerland
- A Primer on Hardware Security: Models, Methods, and Metrics, Masoud Rostami, Farinaz Koushanfar, and Ramesh Karri
- Hardware Security: Threat Models and Metrics, Rostami and F. Koushanfar, Rice University and J. Rajendran and R. Karri, Polytechnic Institute of NYU

- Jia Di, Computer Science and Computer Engineering Department, University of Arkansas and Scott Smith, Electrical and Computer Engineering Department, University of Missouri-Rolla
- Creating a Weapon of Mass Disruption: Attacking Programmable Logic Controllers, Morten Gjendemsjø, Norwegian University of Science and Technology, Department of Computer and Information Science, June 2013
- Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testi, YongBin Zhou, DengGuo Feng, State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences
- Researchers can keylog your PC using your iPhone's accelerometer, Chris Foresman, 2011
- Bad vibrations: How smart phones could steal PC passwords, Kevin McCaney, 2011
- Note on side-channel attacks and their countermeasures, Guido Bertoni, Joan Daemen, Michae¨l Peeters and Gilles Van Assche, The KECCAK Team, May 2009
- Time-Based Blind SQL Injection using Heavy Queries, Chema Alonso, Daniel Kachakil, Rodolfo Bordón, Antonio Guzmán y Marta Beltrán Speakers: Chema Alonso & José Parada Gimeno
- Introduction to Side Channel Attacks, Hagai Bar-El, Discretix Technologies Ltd.
- Hardware Security Course, Coursera and University of Maryland
- Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems, Paul C. Kocher, Cryptography Research, Inc., 1996

קטעי וידאו:

- DEF CON 24 2016 Side channel attacks on high security electronic safe locks
- Introduction to Side-Channel Power Analysis (SCA, DPA)
- Compromising Electromagnetic Emanations of Keyboards Experiment 1/2
- Compromising Electromagnetic Emanations of Keyboards Experiment 2/2
- Cyber Security in Transportation: Hype or Armageddon

מצגות:

- Lecture 14 - Design for Testability, M. Horowitz, Computer Systems Laboratory, Stanford University

- Exploiting the DRAM rowhammer bug to gain kernel privileges, How to cause and exploit single bit errors, Mark Seaborn and Thomas Dullien
- Hacking The IoT (Internet of Things) PenTesting RF Operated Devices, Erez Metula, AppSec Labs, OWASP Israel Meeting 2016

ביבליוגרפיה בעברית:

מאמרים:

- כך תפרצו למחשב הנייד של השכן שלכם בעזרת פיתה, רדיו, וסמארטפון, ירון כהן צמח, דה מרקר, 26.06.2015
- מבוא לשימוש ביכולות Machine Learning בפתרונות אבטחת מידע וסייבר, יובל סיני, גליון 59, מרץ 2015, Digital Whisper
- פרופ' עדי שמיר פיתח שיטה לפריצת הצפנה על ידי האזנה למחשב, עומר כביר, כלכליסט, 22.12.2013
- הרקע המתימטי של RSA, או: איך הצפנת RSA עובדת? בעז (tsabar), גליון 25, אוקטובר 2011, Digital Whisper
- שרלוק הולמס בקו הייצור, עמוס קולט,מנהל הנדסה ותחום USR,חברת DFMA
- אבטחת מידע - תיאוריה בראי המציאות, אלי דיין
- התקפת שיבוש (קריפטוגרפיה)
- התקפת ערוץ צדדי

ספרות:

- מבוא להנדסת מחשבים, מבוא למיקרומחשבים ולמיקרומעבדים, שרה פולק, יעקב שינבוים, ד"ר נונל טירר, המרכז לטכנולוגיה חינוכית (מט"ח), 2015
- מערכות ספרתיות, אריה אילון, יעקב שורץ, אהרון אהרון, המרכז לטכנולוגיה חינוכית (מט"ח), 2009

קטעי וידיאו:

- מערכות ספרתיות עם ליביו - לוגיקה סדרתית חלק 1, יסודות לוגיקה סדרתית והכרת הדלגלג

מצגות:

- Flip Flop, יהודה אפק, נתן אינטרטור, אוניברסיטת תל אביב